S. HRG. 111–333

REAUTHORIZING THE USA PATRIOT ACT: ENSURING LIBERTY

HEARING

BEFORE THE

SUBCOMMITTEE ON ADMINISTRATIVE OVERSIGHT AND THE COURTS

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

SEPTEMBER 23, 2009

Serial No. J–111–49

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

55–610 PDF WASHINGTON : 2010

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

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
BENJAMIN L. CARDIN, Maryland
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
EDWARD E. KAUFMAN, Delaware
ARLEN SPECTER, Pennsylvania
AL FRANKEN, Minnesota

JEFF SESSIONS, Alabama
ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
MATT MINER, *Republican Chief Counsel*

SUBCOMMITTEE ON ADMINISTRATIVE OVERSIGHT AND THE COURTS

SHELDON WHITEHOUSE, Rhode Island, *Chairman*

DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
BENJAMIN L. CARDIN, Maryland
EDWARD E. KAUFMAN, Delaware

JEFF SESSIONS, Alabama
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
LINDSEY GRAHAM, South Carolina

SAM GOODSTEIN, *Democratic Chief Counsel*
MATT MINER, *Republican Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

SUBMISSIONS FOR THE RECORD

REAUTHORIZING THE USA PATRIOT ACT: ENSURING LIBERTY

WEDNESDAY, SEPTEMBER 23, 2009

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC

The Committee met, pursuant to notice, at 10 a.m., U.S. Senate, Committee on the Judiciary, Room 226 Dirksen Senate Office Building, Hon. Patrick Leahy presiding.

OPENING STATEMENT OF HON. PATRICK LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. Good morning, everybody. After September 11th, for many of us it still feels like yesterday, I worked to ensure that the USA Patriot Act included oversight. I think one of the things that as much as we were concerned about that attack, as much as we were concerned about the fact that in many areas we had, we the United States had missed the signs that attack was imminent.

I wanted to make sure that if we were going to increase information gathering powers of the government, that we would sweep in U.S. citizens. I wanted to make sure it was implemented appropriately. This was not a partisan attitude.

I worked with an in-house majority leader, Republican Dick Armey, a very conservative member of the House who agreed with me on this and we included sunsets for some of the provisions with the greatest potential to directly affect Americans. We wanted to make sure that after they had been used for a while, we would be forced to look at them again because they could be reauthorized once we did.

We debated the reauthorization of the Patriot Act for several months in 2005 and 2006. I again worked to protect the civil liberties and constitutional rights of Americans while providing the government with the tools it needs to aggressively go after those people who would harm us.

Now, unfortunately, while the reauthorization bill of 2006 had some improvements, some significant improvements, it lacked sufficient constitutional protections against the authorities granted the government.

I worked with Senator Specter and we were able to expand public transparency in congressional oversight—but in the end several important checks and balances were not included in the final version. While I liked a lot of parts about it, I voted against it because those checks and balances were left out.

Now we have three provisions expiring on December 31st, 2009. It appears because of all the slowdowns we will be in session until December 31, 2009. In fact, I have already made plans. Normally I'd be in Vermont at Christmas which is a nice place to be, but it looks like the way the Senate schedule is going we will be here instead.

We have another chance to get it right. The provisions slated to expire at the end of this year include the authorization for roving wiretaps, the Lone Wolf Measure and an order for tangible things commonly referred to as Section 215, the Patriot Act or the so called Library Record Provision.

In March, I sent a letter to the Attorney General requesting the administration's views on these expiring provisions. Again in June I reiterated that request at a Judiciary Committee oversight hearing. I recently received a letter from the Department of Justice urging Congress to extend the expiring authority.

I also know the President's and the Attorney General's emphasis on accountability and checks and balances and their willingness to consider additional ideas. Actually that openness is something unusual but welcome and I look forward to exploring it.

Yesterday I introduced a bill with Senators Cardin and Kaufman that aims to strike the kind of balance the administration urges. It will extend the authorization—expiring authorization of a new—it will add checks and balances by increasing judicial review of government powers, expand congressional oversight and public reporting on the use of intrusive surveillance measures, and the Leahy/Cardin/Kaufman mandates new audits by the Department of Justice Office of Inspector General on the use of Section 215 and national security letters.

We all appreciate the earlier audits conducted by Inspector General Glen Fine because those led to improvements.

In developing our proposal, I have consulted with Senators Feingold and Durbin. We introduced a more expansive bill last week and with their encouragement I borrowed a few of the accountability provisions from their proposals.

While it is a shared early draft of our proposal, Senator Feinstein, Chair of the Senate Committee on Intelligence, I look forward to working with everybody. We will turn to the issue of our committee meeting on October 1st which is a week from tomorrow.

I am pleased that the Attorney General is moving in the right direction to better control assertions of the state's secrets privileges after our efforts over the last several years to bring oversight and accountability to the administration's invocation of this privilege.

The administration's policies that are being announced right now heckle the Senate legislation we have been passing. It is being announced now and the administration leaked them last night and actually I'm pleased with them.

The Attorney General's announcement incorporates several concepts drawn from our State Secrets Protection Act such as the adoption of a significant harm standard, the creation of new internal controls, the requirement the Attorney General personally approved, the assertion of the State Secret privilege.

I press hard to shine a light on the misuse, there has been a misuse to the State Secret privilege. We want the privilege but we

don't want to misuse. We have to have mechanisms to guide this application. Today's announcement marks progress.

I will closely monitor the implementation of this new State Secret policy. I will make sure everybody has a higher level of accountability and transparency. I am especially concerned with ensuring the government makes a substantial evidentiary showing to a public judge in asserting the privilege so that the rule of the court can be there and determine whether it should be allowed.

I commend the Attorney General, I commend him very highly for working with us and shaping these approved policies and procedures. I am going to yield to Senator Sessions and then we will go right to David Kris and Glenn Fine. Go ahead.

STATEMENT OF JEFF SESSIONS, A U.S. SENATOR FROM THE STATE OF ALABAMA

Senator SESSIONS. Thank you, Mr. Chairman. Thank you for this hearing. You have been a strong supporter of the Patriot Act. It has been a bipartisan act. I do believe that this committee after 9/11 fulfilled its responsibility by carefully scrutinizing every single word in it to make sure that there were no abuses of constitutional rights of our citizens. I think that was achieved.

I don't believe that subsequent events have proven that there have been any abuses of the Act to date and I think in fact the history of the Act shows that it has been very helpful in allowing us to go now some 8 years without having another attack. I appreciate the work that everybody put into this when you were either Chairman and ranking member I guess throughout the whole process. Chairman, I suppose.

Chairman LEAHY. Both.

Senator SESSIONS. Both I guess.

Chairman LEAHY. Of the two I will tell you later which I enjoyed more.

Senator SESSIONS. The provisions of this Act did not create new or unusual powers for the Federal Government. Rather, the Act extended to our National Security Agency the same tools essentially that had long been available to domestic law enforcement that I used as a Federal prosecutor.

In the fight against terrorists, it is only fair and common sense and reasonable that we have at our disposal abilities that have existed for decades to pursue drug dealers and mobsters.

When this Act was passed in 2001 and then reauthorized in 2005, some were concerned that significant violations of civil liberties would result. Some were concerned that libraries would be abused. Well, we have closely examined the performance of our law enforcement agencies under the Act and we can safely say those fears did not materialize.

Our national security and law enforcement agencies have made responsible use of these tools and at the same time continued to protect the safety of the American people.

Three of these essential tools are up for reauthorization. We have the roving wire taps, the business records provision Section 215 and the Lone Wolf section of the Intelligence Reform Act that the Chairman mentioned.

It is important to say at the outset that the administration is requesting that the provisions be renewed. The Assistant Attorney General has written the Chairman that the DOJ has discussed these provisions with the Director of National Intelligence. They are unequivocal about the administration's position that we are still at war with Al Queda and that these provisions should be reauthorized because they are important tools in this war and to make America safe.

The roving wire tap is a provision that prevents terrorists from evading surveillance. Before September 11, 2001, a target could just switch phones several times and the National Security Agency would have to obtain a new court order to have a wire tap on each one of those phones. As a matter of fact, criminals today use phones regularly and they throw them away.

Narcotics and organized crime prosecutors can apply for and are able to apply for roving wire taps so that their agencies could monitor criminals bent on avoiding detection. That was passed in 1986. It allowed that in drug cases.

The provision of the Patriot Act grants terrorist hunters the same tools to catch a savvy terrorist as law enforcement has been using to capture criminals.

FBI Director Muller appeared before us last week and testified since the roving wire tap was authorized, it has been used approximately 140 times. He described this as tremendously important. It is essential given the technology and growth of technology that we have had.

The Business Records Provision Section 215 feels the gap in national security intelligence gathering and according to the Department of Justice has proven valuable in a number of contexts. It permits the authorities to seek permission from courts, go to court to gain access to business records that can help "connect the dots" in tracking terrorists and foreign agents.

When the Act was passed in 2001 and reauthorized in 2005, some feared it would be abused. Well, now we have several years of tracking this and no such incident has occurred. This provision simply extends to national security agents the same abilities basically possessed by any Federal prosecutor.

In investigating ordinary crime, a prosecutor can issue a Grand Jury subpoena which orders the production of all sorts of business records and documents. In fact, ordinary Grand Jury subpoenas are not as regulated as this because they do not need to be approved by a judge as these types of orders are.

As Director Muller told us, these orders have been used about 250 times and "the records that are received are absolutely essential to identifying other persons who may be involved in terrorist activities."

The Lone Wolf section of the Act is a common sense provision that we need to continue the fight against terrorism in the 21st Century even though it has not even been used one time yet; it is there to defend against a very real possibility.

A rogue terrorist may not be linked to a terrorist group. Or if he is, he may not be proven to be linked. In the past, the law required that the National Security Agency show a connection between a terrorist and a terror group or a foreign national power in order to

monitor them. This meant that if a terrorist or a foreign agent left a terror group, abandoned them, perhaps because of a dispute, we would not be able to track him until he joined some other group.

As our armed forces fight and succeed against terror groups, we will inevitably splinter them, perhaps causing some to strike out on their own, or some will self-radicalize, gaining fame from the internet.

The statutory language of this provision is narrow and guarantees that it will not be abused and—the provision stands waiting to be used and has never been used.

The DOJ notes, "we believe that it is essential to have the tool available for the rare situation in which it is necessary rather than to delay surveillance of a terrorist in the hopes that necessary links could be established."

So I believe that Congress and the President work together very well to pass this Act in 2001 and reauthorize it in 2005. Chairman Leahy is a strong believer in civil liberties. You monitored the Act very, very carefully before you lent your support to it. I think it has proven to be valuable and proven not to have been abused. I think it should be reauthorized without any weakening of it. Thank you, Mr. Chairman.

Chairman LEAHY. Thank you very much. Our first witness is David Kris, who currently serves as the Assistant Attorney General for National Security.

Earlier in his career he worked for 8 years as a Federal prosecutor in the Criminal Division. Certainly the ranking member and I are always delighted to see prosecutors here.

He served as Associate Deputy Attorney General and in 2003 supervised the government's use of the Intelligence Surveillance Act.

Now Mr. Kris, as you know, some of us in this committee worked very hard to ensure your confirmation to a vital position within the administration. None of the policies being announced today by the Attorney General with regard to government claims the State Secret privilege, you are going to have a very critical role to play. We are going to be looking for you to fulfill that role in the new policy by ensuring against misuse and overuse—the State Secret, but also I think by making sure the proper role of the court is respected.

So Mr. Kris, Assistant Attorney General Kris, please go ahead, sir.

STATEMENT OF DAVID KRIS, ASSISTANT ATTORNEY GENERAL, WASHINGTON, DC

Mr. KRIS. Thank you, Chairman Leahy, Senator Sessions and members of the committee, thank you for inviting me to testify today.

As you know from my written submission in the letter that we sent on September 14th, we favor reauthorization of the three sunsetting provisions in the USA Patriot Act and we are open to working with Congress on those provisions.

We have seen recent draft legislation from Senator Leahy, Senator Feingold and others and we are reviewing those drafts now. Of course we don't have a position on them at this time.

Let me just walk through each of the three provisions quickly. The first is the roving surveillance provision. As you know, this

was enacted in 2001 to correspond to preexisting authority that applies to law enforcement surveillance. I want to make two basic points about this roving surveillance provision.

The first is that we can obtain roving surveillance authority from the court only when we can show to a judge that the actions of the surveillance target, the person or entity from or about whom we are seeking information may have the effect of thwarting our ability to conduct the surveillance with the aid of a specific third party like a telecommunications provider. So we have to show this thwarting effect first.

Let me try to explain how that thwarting effect can occur. In an ordinary FISA surveillance case, the government shows probable cause to the judge of two basic facts. First that the target is a foreign power or an agent of a foreign power, and those terms are defined in great detail in the statute.

Second, that the target is using or about to use a particular facility like a 10 digit telephone number or something like that.

For its part then the court issues two orders. First, a primary order to the government that says yes, you are authorized to do this surveillance, and then what is called a secondary order directed to the particular telecommunications provider or other third party and that secondary order says you should help the government effectuate the surveillance. The phone company needs to help us do the surveillance on the particular phone number.

If in an ordinary FISA case, the target switches carriers from one provider to another, the new provider will not honor a secondary order that was directed only at the old provider. You wouldn't want it any other way. You wouldn't want phone company number 2 to start honoring orders that are directed at phone company number 1.

So that is where the thwarting can occur because we have to go back to court, file a new pleading and get a new order. That creates a gap in our coverage.

In a roving case we avoid that problem because we get in effect a generic secondary order that can be served on any provider so that we can follow the target from provider to provider if he jumps around.

That is the first point I wanted to make about this provision. The second point which comes at the back end of roving and is equally important and that is whenever we implement this roving authority, we must report to the court, to the FISA court normally within 10 days of the probable cause that ties the target to the new facility that he has roamed to. That if you think about it makes sense because the main thing that changes in a roving surveillance case, in effect really the only thing that typically changes is the new facility.

The target is the same target. The probable cause that the target is an agent of a foreign power is the same probable cause. So the statute I think wisely and correctly focuses on what is new and that is the probable cause linking the target to this new facility. So that is the way the architecture of the statute works and that is essentially why we think it should be renewed.

I should also add that I'm not aware of any major compliance problems with the implementation of the roving authority since its inception in 2001.

Briefly with respect to the Lone Wolf provision which is the second of the three, this provision has never been used. Again, I have sort of two quick points. The first is as to its scope. This is a provision that applies only to non-US persons, not to US citizens, not to green card holders, and only when they themselves engage in or prepare to engage in international terrorism.

The provision is designed basically to address the possibility of the situations that Senator Sessions described. A person who self-radicalizes and engages in this international terrorism without being a member of any group or a person who was a member but then breaks with a group and then goes off on his own as a kind of free agent.

If that kind of case arises, we would have difficulty establishing or maintaining our coverage without the Lone Wolf provision. That is the idea behind it.

Third and finally the business records provision Section 215 of the Patriot Act. In general, this provision is used when three circumstances exist. First, the information sought can't be obtained by a national security letter. National security letters exist for specific types of information in specific situations.

Second, a Grand Jury subpoena would not be sufficiently secure secret, and third, the provider either can't or won't turn it over voluntarily. So with that, I will stop and I look forward to answering your questions. Thank you.

Chairman LEAHY. Thank you very much. I am holding the National Security Investigations and Prosecutions which you co-authored with Douglas Wilson. So if there is anything you disagree with what you have in there, be prepared.

Glenn Fine is well known of course as the committee he served as the Department of Justice Inspector General since 2000. He has been a member of the Office of the Inspector General since 1995.

His office conducted comprehensive audits of Section 215 of the Patriot Act of the use of national security letters. These audits which are combined with a number of other reports issued by his office represented really the largest portion of the public reporting on the use of surveillance authorities.

Mr. Fine, glad to have you here. Go ahead, please.

STATEMENT OF GLENN FINE, INSPECTOR GENERAL, WASHINGTON, DC

Mr. FINE. Mr. Chairman, ranking member Sessions, members of the committee, thank you for inviting me to testify about the Office of the Inspector General's work related to the Patriot Act.

Our most significant reviews have focused on the FBI's use of national security letters and Section 215 orders. Pursuant to the Patriot Reauthorization Act, in March, 2007 and March, 2008, we issued reports examining the FBI's use of these two authorities and I will focus my testimony on our findings from those reviews.

First, with regard to the use of national security letters, NSLs. Our reports recognize the major organizational changes the FBI

was undergoing in this counter terrorism and counter intelligence efforts during this period.

Nevertheless, our reports found that the FBI had engaged in serious misuse of NSLs. For example, we found that the FBI had issued many NSLs without proper authorization and had made improper requests under the statutes cited in the NSLs. Most troubling, we identified more than 700 instances in which the FBI improperly obtained telephone toll billing records by issuing so called exigent letters.

These letters stated that they were being issued due to exigent circumstances and that the FBI was in the process of obtaining subpoenas for the requested information.

In fact, we found that many of these letters were not issued in exigent circumstances and that subpoenas had in many instances not been submitted to the U.S. attorney's offices as represented in the letters.

As a result of our findings, the FBI has ended its practices of using exigent letters and the OIG is now in the final stages of completing a review, examining who is accountable for the misuse of these letters.

In total, the OIG's two reports on national security letters made 27 recommendations to the FBI to ensure that it uses NSLs in accordance with the requirements of law, department guidelines and internal FBI policy. We believe that the FBI has taken these recommendations seriously and has devoted substantial time and resources to implementing them.

For example, the FBI created an Office of Integrity and Compliance to identify risk areas in FBI programs. However, we have some concerns about the staffing of this office and we also do not believe that this office should be looked to as the primary oversight mechanism to ensure that the FBI uses NSLs properly.

Because of the emphasis the FBI has placed on this office, the OIG intends to initiate a separate review to assess in detail the work of the office. In addition, in response to our reports, the department established a national security letter working group to develop minimization procedures regarding acquisition, dissemination and retention of information obtained from NSLs. Yet while this group has drafted proposed recommendations, these recommendations have not yet been finalized even though it has been more than 2 years since our first NSL report was issued.

We believe the department should complete its review of the working group's proposals and promptly issue final minimization procedures for NSLs.

With regard to the use of Section 215 orders, the OIG examined and issued two reports on the FBI's use of these orders to obtain business records. While used much less frequently than NSLs, the FBI believes that the Section 215 authority is essential to national security investigations because it is the only compulsory process for certain kinds of records.

Our reviews did not identify any illegal use of Section 215 orders. However, a second report does discuss a case in which the FISA court twice refused to authorize a Section 215 order based on concerns that the investigation was premised on protected First Amendment activity.

The FBI subsequently issued NSLs to obtain information about the same subject based on the same factual predicate even though the NSL statute contains the same First Amendment caveat as the Section 215 statute.

My written statement also describes other reviews within the FBI that while not directly involving Patriot Act authorities, relate to FBI programs and functions that can impact its ability to perform its vital mission.

In conclusion, we found that the FBI did not initially take seriously enough its responsibility to ensure that Patriot Act authorities such as national security letters were used in the court with the law, Attorney General guidelines and FBI policies.

Since issuance of our reports, however, we believe that the FBI has devoted significant effort to correcting its misuse of these authorities. Yet we believe this is an ongoing process and is too early to conclude definitively that the FBIs efforts have fully and finally eliminated all the problems we found.

We also believe that as Congress considers reauthorizing provisions of the Patriot Act, it must ensure through continual and aggressive oversight mechanism that the FBI uses these investigative authorities appropriately.

We recognize that the OIG has an important role to play in this oversight process and we intend to continue our reviews of the FBI's use of these authorities.

That concludes my testimony and I would be pleased to answer any questions.

Chairman LEAHY. Thank you very much, Mr. Fine. The bill I introduced this week, the USA Patriot Act Sunset Extension Act has a 4-year sunset in all the three expiring Patriot Act provisions similar to what we did in 2001 and again in 2005/06 reauthorization.

But it also has a new 4-year sunset on the use of national security letters. These are the letters that allow the government to obtain bank records and credit card statements, medical records and other personal information all without a warrant.

Given the misuse of the NSL authority that was seen in the Inspector General's 2007 report, I thought it was time to take another look at the authority. So I introduced the USA Patriot Act after September 11th. I said because I thought we needed these aggressive tools and I was glad to do it.

But given that these authorities allow the government to collect so much information about Americans, is it the administration's position, do they agree with me that it is only reasonable to have a sunset on these authorities because it would force us to periodically look at them and see how they are being used?

Mr. Kris.

Mr. KRIS. Senator, thank you. Obviously as I mentioned, we don't have an official administration position on that element of your bill or the others. It is certainly something we can think about and discuss and work with the committee.

Chairman LEAHY. Let me ask Mr. Fine.

Mr. FINE. Well, I don't speak for the administration here. I do think it's important to ensure that there is aggressive oversight of

this, that it be continually looked at. Our audits did expose problems in NSLs and it is important to continue that review.

Chairman LEAHY. Let me put it this way. Has it been your experience that there is more oversight at the time when sunset provisions are about to kick in?

Mr. FINE. There is more scrutiny of the issues as evidenced by this hearing. That's clear.

Chairman LEAHY. Now, Section 215, the business records orders has an incredibly expansive authority. As long as the government meets the simple relevancy standards of things sought pertaining to a specific kind of intelligence along investigation, the FISA court can allow them to take not just business records, but any thing. That means not just library records but the lawful purchase of firearms, something of some concern in my own state of Vermont, your own personal medical records of some concern to all of us, your computer, any tangible thing at all even if it meant it closed down your small business.

The government is almost always guaranteed success because current law confers a presumption of relevance to the government's claim that what it is seeking is relevant to the investigation.

It is quite an advantage to the government. You are a small business and somebody comes in and just swoops up and takes out all your computers and you are effectively closed down. Then you say well, there is a presumption of relevance.

I would think as technology advances and more and more personal information is available, isn't it reasonable to require the government to have to at least prove the things that it is seeking are relevant in terrorism investigation and connect it to at least a suspected terrorist before they are allowed to go into all this huge amount of private material?

Mr. Kris.

Mr. KRIS. The statute requires the statement of fact showing that there are reasonable grounds to believe that the tangible things sought are relevant.

Chairman LEAHY. But there is automatically a presumption.

Mr. KRIS. No, I understand that there is a presumption if the materials pertain to a foreign power or an agent of a foreign power or the activities of the agent of a foreign power. In certain categories there is a presumption, but nonetheless, there does have to be a statement and then a showing of relevance.

If you think about how this kind of authority is used and the stage at which it is used. It is used at an early stage often of an investigation to gather documents not after probable cause has been established, but in order to establish probable cause or in order to weed out people who really don't belong in the investigation.

Chairman LEAHY. It is ordinarily expansive. If you have somebody in there who just wants to do it because they don't like somebody for example, on business, they could close down the business. If they wanted to do a fishing expedition in hospital records, everybody's records, yours, mine, everybody else's, they can do that and they are given a presumption of relevance.

Mr. FINE. Well, obviously there is here a provision that prohibits the use of this against someone based solely on their exercise of

First Amendment rights, so some of these cases where you posit some very bad hypotheticals would be just flat out prohibited by the statute. I should also say that——

Chairman LEAHY. I wasn't speaking about First Amendment matters.

Mr. FINE. And I should also say that the recipient of a 215 order who may not always be the person whose records are in play has a right to bring an action in the FISA court. That hasn't happened. I think that may be an indication of how the recipient——

Chairman LEAHY. How do they bring it? They have to overcome presumptions. I mean, the cards are rather stacked.

Mr. FINE. I mean, I don't disagree with you insofar as the relevance standard with or without the presumption is not a very high standard. It isn't a probable cause standard or proof beyond a reasonable doubt or anything of the sort.

I think that reflects the fact of how this investigative tool is used and indeed on the criminal side, if you think about the standard that applies to a Grand Jury subpoena under the R. Enterprises case, the Grand Jury has enormous authority without a judge signing off on the subpoenas to collect a lot of information under a very low standard as well and that is just the way investigative tools are structured.

Chairman LEAHY. You and I are going to be talking about this.

Mr. FINE. I look forward to that.

Chairman LEAHY. Also the bill I introduced with Senators Cardin and Kaufman include new audits on Section 215 orders for tangible things in the use of national security letters—trace devices.

Given the letter's favorable language to us, the letter you sent to me on reauthorization, speaking about congressional oversight, do you support the audits in the bill?

Mr. FINE. As I said, we don't have a position on anything particular yet. I do want to say, though——

Chairman LEAHY. I mean, your letter says you support oversight. Are you saying that you support oversight but you can't take a position on oversight?

Mr. FINE. I mean, I'm not in a position to announce an administration position on any particular aspect of your bill. The bill obviously was dropped fairly recently. We are looking at it now actively and we are interested in working with the committee and with you and others to try and see if these tools can be sharpened.

Chairman LEAHY. On these audits, would you get back to me as quickly as possible?

Mr. FINE. Yes.

Chairman LEAHY. Thank you. Senator Sessions.

Senator SESSIONS. Thank you. Mr. Kris, isn't it true that a Federal drug enforcement agent who is investigating a drug organization can issue administrative subpoenas without a court or a Grand Jury oversight and obtain telephone toll records or motel records or even bank record relating to that investigation?

Mr. KRIS. Yes, there are a number of administrative subpoenas including in the drug arena and other areas that operate as you——

Senator SESSIONS. Well, how about an IRS agent who is investigating tax fraud? Can they get your bank records and your telephone toll records?

Mr. KRIS. Yes. Under certain circumstances they can, and you are right, there is an array of circumstances.

Senator SESSIONS. Isn't it true that the national security letters really have more oversight and more requirements on them perhaps than the administrative subpoenas that other Federal agencies have been using for many, many decades?

Mr. KRIS. It is certainly true that a 215 order has more process associated with it than these criminal side collection authorities because a 215 order is issued by a judge based on an application made by the government in advance of the issuance of the order and the production of the tangible things.

The authorities that you were just reciting on the criminal side including the Grand Jury subpoena don't require advanced judicial approval.

Senator SESSIONS. Now, just for our members and those that might be interested, documents in the possession of a bank or a telephone company are not in the possession of the defendant. That is a third party.

Hasn't it been true that the court has always recognized as a different standard in the burden of proof when you obtain information from a third party than getting it out of your desk drawer or coming out of your pocket or your automobile where you have personal control over it?

Mr. KRIS. I mean, that is certainly correct both with respect to the Fourth Amendment and in some cases under active production to the Fifth Amendment. When you give information to a third party, the Fourth Amendment calculus changes under the Miller decision from the Supreme Court.

Senator SESSIONS. Because essentially the telephone toll records or the bank records are in possession of somebody else. Everybody at the bank, everybody at the phone company has access to those records. You have a diminished expectation of privacy in records held by other institutions than held by yourself.

Now, with regard to the roving wire taps, isn't it true that you still have to have and you still have to go through the very significant process to obtain a warrant to have that approved by a Federal judge and they have to set forth extensive factual predicates to justify the court issuing that warrant and it is quite extensive and quite a major operation to get a Federal tap on a telephone whether it is one phone or a roving phone.

Mr. KRIS. I mean, both under Title 3, the Criminal Wire Tapping Statute and under FISA, there are lengthy applications that are prepared on the FISA side by attorneys in my office. I signed some of those, so yes, they are extensive. They have to make a showing of probable cause that we make in every case.

When we want to seek roving authority, we have to make an additional showing about the actions of the target thwarting or having a possibility of thwarting the surveillance.

Senator SESSIONS. And there has been no lasting of that in national security cases that you would have in a mafia case, an organized crime case, a case of that nature.

Mr. KRIS. I mean, the statute is different under FISA than it is under Title 3 on the criminal side. But the probable cause requirements that have been in FISA since 1978 have not been watered down.

Senator SESSIONS. It seems to me that is the fundamental protection that every American has is that before you can listen in on your phone conversation, you have to have probable cause that a crime is underway, that this person is involved with it and this telephone or a telephone may be utilized in the furtherance of it, isn't that right?

Mr. KRIS. On the criminal side, yes, you would make a showing of a specific crime. Not every crime will do. They have to have several listed in 2516 of Title 18 and then the facility the phone would say is being used in connection with that crime.

Senator SESSIONS. Well, Mr. Fine, you wouldn't dispute the thousands and thousands of administrative subpoenas issued by the IRS to find out if we paid our taxes or DEA investigating drugs, would you? You acknowledge that?

Mr. FINE. I acknowledge that, yes.

Senator SESSIONS. Well, let me ask you this, Mr. Fine. With regard to the complaints you raised initially, you have indicated still the FBI has not gotten its act totally together which I am not happy with. I think they should respond and follow these rules as strictly as they possibly can. But the national security letters are not in essence much different than the administrative subpoenas issued by other Federal agencies, are they? For the most part, the ones that are issued most often.

Mr. FINE. They are similar but the are broader. There is more of them. They are issued in more contexts and we found in our particular scrutiny of this that they were not used properly and that they had not followed their own policies, that they were used sometimes in excess of the statutes.

Senator SESSIONS. Have you issued your final report on that?

Mr. FINE. Well, this is our March, 2007 and March, 2008 reports on national security letters, yes.

Senator SESSIONS. Have we seen that report?

Mr. FINE. Yes.

Senator SESSIONS. Well, to what extent have your recent evaluations discovered that the FBI is still not following proper procedures?

Mr. FINE. We issued these reports in March, 2007 and in March, 2008 we issued a follow-up report and found that they had taken substantial efforts. They had made significant strides but there still needed to be more work done.

We have not issued a report since then but we have been in contact with them and we anticipate a continuing oversight over this matter.

Senator SESSIONS. Well, I think that's fine, but some of the errors were like the agency had used a U when they should have used a subsection B and more clerical errors that you counted correctly as being errors, is that correct?

Mr. FINE. There were a whole range of errors. Some were clerical errors, some were errors by the telecommunication providers, some

were errors by the agency, some were serious errors where they were issuing NSLs in instances when they were not proper.

Senator SESSIONS. Thank you.

Chairman LEAHY. Thank you very much.

Senator Feinstein.

Senator FEINSTEIN. Thank you very much, Mr. Chairman. Thank you for the bill. Gentlemen, welcome. I'd like to put on my other hat which is Chairman of the Intelligence Committee.

There was so much criticism after 9/11 that the intelligence community really didn't know where an attack would take place or was able to put together certain facts that would lead to an arrest that would prevent an attack. So since that time we have seen a greatly developed intelligence community aimed at protecting the homeland which I very much appreciate.

We are in the process of a major intelligence investigation in both New York and Colorado. I happen to believe it is a real investigation and I know that the FBI has enormous resources expended in this investigation.

Mr. Kris, I would like to begin with this question. Is there anything in this bill that would impede or affect the present investigation?

Mr. KRIS. Senator, thank you for that question. I think the best answer to that is that that is something that would properly be discussed in a classified setting and I think we would be happy to do that.

Obviously we are not going to discuss classified matters here, and also there is this Justice Department policy about commenting on ongoing investigations. So I think for both of those reasons, that will be deferred to a different setting, but I appreciate the question.

Senator FEINSTEIN. Well, then clearly your answer is not no, so I think we ought to have that——

Chairman LEAHY. I think in fairness to Mr. Kris, his answer is what his answer was.

Senator FEINSTEIN. All right. Well, thank you very much but I am free to interpret it however I might choose to and I certainly think we should have that classified session.

Can you describe what types of information would be included in a statement of fact? I am now talking about the NSL provisions of this bill. How much detail would have to be in the statement of facts in order to prove relevancy?

Mr. KRIS. Do you mean under Senator Leahy's bill?

Senator FEINSTEIN. That's correct.

Mr. KRIS. I want to be very cautious about commenting on it because we just haven't worked all the way through the bill to figure out what it would actually mean. It is complicated stuff, as you know.

If we are changing the standard in a significant way, then it will by definition, and I think it is designed to, have an effect on the way the authorities are used and that is a question of striking a balance as to how much authority you want to give. But we haven't as an administration yet worked through at that level of detail exactly what the implications would be here.

Senator FEINSTEIN. So could you answer the question? Would the information in a statement of facts be classified? And if so, how

would private sector companies be expected to handle that information?

Mr. KRIS. I'm not sure I understand, Senator. There is a provision I think I have read that would require us to explain to private sector entities, telecom providers or others exactly what our basis is. That would be a change I think in current law. Again, we are still trying to work through that and figure out how it would work, so I don't want to announce or take a position on it. I think I understand that is what you are referring to. That would be a change.

Senator FEINSTEIN. The Leahy bill would add a requirement for the statement of fact which would show reasonable grounds to believe that the information sought is at least relevant to an authorized investigation. Would you have a problem with that?

Mr. KRIS. Again, I think that's a position we would like to work through in an orderly fashion and then deliver to the committee once we have done that homework. I apologize that I'm not in a position to announce an administration position here.

Senator FEINSTEIN. OK. You laid out certain tangible things sought under the business records section as presumptively relevant if the government shows that they pertain to a foreign power, an agent of a foreign power, the activities of a suspected agent of a foreign power who is the subject of an authorized investigation or an individual in contact with or known to an agent of a foreign power who is the subject of such investigation.

The bill as I understand it removes the presumption of relevance described above and it requires the government to show relevance. Can you describe how the government would be expected to show relevance? Would this also require a statement of fact to a court? And how much detail would be required?

Mr. KRIS. I will answer that question carefully so that I don't get into anything classified or operational. But yes, I mean, the statute currently requires a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant.

So today we are making a statement of fact to a judge. We would be aided by the presumption that you just described if the conditions of that presumption are satisfied, if that presumption is eliminated then we won't have that benefit of the presumption. We are still going to be making a statement of fact.

What that would be would vary from case to case as you can imagine. But when you are making a statement of fact in support of a showing of relevance, you are trying to show the judge why it is that this information that you are seeking pertains to or is important to the investigation that you are undertaking.

Senator FEINSTEIN. So you do not see this as slowing down an investigation? It could be done in a very timely way?

Mr. KRIS. Well, under 215, obviously Mr. Fine has written extensively about the delays associated with the use of 215 in the past. I think we have made improvements on making it faster. When you change the bill, if you change the law, it may have an effect. We just haven't sort of worked through in every detail exactly what those changes would mean operationally yet.

Senator FEINSTEIN. Thank you very much.

Chairman LEAHY. Thank you, Senator.

Senator Feingold.

Senator FEINGOLD. Thanks, Mr. Chairman. I'm glad the committee is moving forward on Patriot Act reauthorization. I introduced legislation along with Senator Durbin and eight other senators that takes a comprehensive approach to fixing the USA Patriot Act and the FISA Amendments Act.

It permits the government to conduct necessary surveillance but within a framework of accountability and oversight. I understand as you indicated, Mr. Chairman, of course that you have also introduced legislation. I look forward to working with you closely on these issues.

I have a full statement that I ask be placed in the record.

Chairman LEAHY. Without objection.

Senator FEINGOLD. Thank you, Mr. Chairman. I also ask that letters in support of the Justice Act bill that we have introduced be placed in the hearing record as well.

Chairman LEAHY. Without objection.

Senator FEINGOLD. Mr. Kris, let me start by reiterating something you and I talked about previously, and that is my concern that critical information about the implementation of the Patriot Act has not been made public. Information that I believe would have a significant impact on the debate.

I urge you to move expeditiously on the request that I and others in this committee have made before the legislative process is over.

Now, in Suzanne Spaulding's testimony for the next panel, she argues that additional safeguards are needed in the context of intelligence investigations because of the very broad scope of intelligence investigation. The secrecy with which they must be conducted and the fact that they often do not lead to prosecution. That is, we have to take into account that safeguards inherent to criminal investigations are simply not always present in the context of intelligence investigations.

Mr. Kris, do you agree that additional vigilance is needed in the context of intelligence investigations?

Mr. KRIS. Yes.

Senator FEINGOLD. And in fact isn't that what was demonstrated at least in part by the IG reports on national security letters?

Mr. KRIS. Well, I think the problems that Mr. Fine found are significant. I think they have been remedied. I'm not sure that those are inherent in an intelligence use of NSLs, but, I mean certainly they are significant and they warrant attention and I think they have gotten a lot of attention.

Senator FEINGOLD. Mr. Fine, would you agree that the lack of safeguards contributed to the misuse of NSLs?

Mr. FINE. I think to some extent the fact that they were not transparent does produce an environment where there needs to be more significant vigilance.

Senator FEINGOLD. Mr. Kris, as you know, the Patriot Act provided statutory authority for the government to obtain that special sneak and peak, criminal search warrants that allow agents to break into American homes and conduct secret searches without telling them for weeks, months or even longer.

It is true, isn't it, that these searches can be conducted also in run of the mill criminal cases and do not require any connection to terrorism?

Mr. KRIS. That's true, both before and——

Senator FEINGOLD. In fact, according to a July, 2009 report of the Administrative US courts, isn't that exactly how this authority has most recently been used?

The report shows that in fiscal year 2008, sneak and peak search warrants were requested 763 times but only three of those initial requests, just three, were in terrorism cases? The vast majority were for drug cases.

Now, is that your understanding of that report and does it concern you at all?

Mr. KRIS. It is my understanding and I want to say thank you to your staff who alerted me and allowed me to read the report in advance of this hearing. It does say here that 65 percent of the, these are criminal sneak and peak were in drug cases.

Obviously just to make something clear which I know you understand, but on the FISA side, the searches that we do pursuant to FISA are not exactly sneak and peak. They are generally covert altogether. So this authority here on the sneak and peak side on the criminal side is not meant for intelligence, it is for criminal cases.

I guess it is not surprising to me that it applies in drug cases.

Senator FEINGOLD. As I recall, it was in something called the USA Patriot Act which was passed in a rush after an attack on 9/11 that had to do with terrorism. It didn't have to do with regular run of the mill criminal cases.

Let me tell you why I'm concerned about these numbers. That is not how this was sold to the American people. It was sold as stated on DOJ's website in 2005 as being necessary 'to conduct investigations without tipping off terrorists.'

I'm going to say it is quite extraordinary to grant government agents the statutory authority to secretly break into American's homes in criminal cases and I think some Americans might be concerned that it has been used hundreds of times in just a single year in non-terrorism cases and that is why I am proposing the additional safeguards to make sure that this authority is available where necessary but not in virtually every criminal case and also to shorten the time period for notification.

Mr. KRIS. Well, I don't mean to quibble with you. I do want to just point out one thing which is before, and I was trying to carve out FISA, just to clarify that FISA is a different authority where it is covert, and also it puts, if I am correct on this, I believe two Courts of Appeals prior to the Patriot Act had authorizes sneak and peak under existing law. This was meant to be a codification of that doctrine.

Senator FEINGOLD. Some courts permitted secret searches in limited circumstances before the Patriot Act as I remember, but they also recognize the need for notice unless a reason to continue to delay notice and it was demonstrated and they specifically said that notice had to occur within 7 days which is what we fought for at the time of the Patriot Act which is what our bill proposes.

So I think you make a fair point that it was allowed to some extent. But without these protections, this is a dramatic change in

our general criminal law that doesn't necessarily relate to terrorism. Thank you, Mr. Chairman.

Chairman LEAHY. Do you want to respond to that, Mr. Kris.

Mr. KRIS. Well, I was just going to sort of support Senator Feingold's conclusion by saying that this report says the periods of delay range from 3 days to 365 days with 90 days being the most common period. So just based on the report you provided.

Chairman LEAHY. Thank you. Senator Durbin.

Senator DURBIN. Thanks, Mr. Chairman. My first run-in with librarians was at a very early age when they were infringing on my personal liberties in the East St. Louis Public Library in telling me to shut up and now librarians have taken a different role when it comes to individual rights and liberties on the national stage.

It has become very vocal in considering the impact of some of our conversation on the privacy of individuals who use libraries. It led to former Attorney General Ashcroft characterizing librarians as hysterics and he went on to say that the Department of Justice has neither the staffing, the time nor the inclination to monitor the reading habits of Americans. Former Attorney General Gonzales said something along the same lines.

In your testimony, Mr. Kris, about Section 215, you said it has not been used to 'collect sensitive personal information on constitutionally protected activities such as the use of public libraries.'

However, we do know that under the previous administration, the Justice Department issued national security letters for the library records of innocent Americans. Isn't that true?

Mr. KRIS. Actually, I won't dispute you on that, but I don't have a specific recollection of that.

Senator DURBIN. I think it is accurate. What I would like to ask is what is the Justice Department's current policy on using national security letters on libraries?

Mr. KRIS. Well, as you know, Section, now are you talking about national security letters or 215? Because national security letters unless I'm having a moment here, don't get sent to libraries. It is, you know, RIPA, FICRA, those are specific financial. So I think you mean 215 orders.

Senator DURBIN. There was testimony before our committee, George Christian?

Mr. KRIS. Oh, you probably meant a 2709 letter.

Senator DURBIN. A librarian who received an NSL for library records.

Mr. KRIS. I understand. I'm sorry. I did have a moment there. I'm sorry.

I mean, if it is within the ambit of statute, then I think we might use the statute in that way and there have been cases, I can think of an espionage case, a terrorism case and a conventional murder case I believe in which libraries have been used.

Section 215, which is what I mistakenly thought you were referring to obviously expressly can apply to a library, hasn't been used that way but could be. You wouldn't I think want to declare a library a safe zone.

Senator DURBIN. No, but in your words you called sensitive personal information on constitutionally protected activities such as the use of public libraries.

VerDate Nov 24 2008 14:15 Apr 06, 2010 Jkt 055610 PO 00000 Frm 00022 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\55610.TXT SJUD1 PsN: CMORC

The Patriot Act allows the FBI to issue NSLs for sensitive personal information on innocent Americans, not just those that we have connected up or believe we can connect up to terrorist activities without a demonstration of that connection.

As Mr. Fine has reported, the standard for issuing an NSL is "can be easily satisfied." For example, if an FBI field office wanted to identify someone who used an internet terminal at the Chicago public library, they could issue an NSL for the internet and email records of the library including the records of hundreds of ordinary innocent citizens.

Now, we are talking about changing that for obvious reasons since as you characterize it and I agree, we are dealing with constitutionally protected activity.

Would you agree that under current law, the Justice Department cannot guarantee innocent Americans that their library records, their activities, internet terminals and libraries for example are safe when the law allows the FBI agents to obtain these records without the approval of the Department of Justice and without any connection to a suspected terrorist act?

Mr. KRIS. Well, I wouldn't put it the way you just put it, Senator Durbin, but I take your basic point which is that there are statutes that allow this. Also on the criminal side, you know, Grand Jury subpoenas could be directed at libraries and have been. So the nature of an investigation at that stage is that the government has to sweep more broadly than just the individual who may end up being the defendant or identified as a terrorist precisely because they are trying to develop the case.

So that is how I think I would put it. Not quite the way you put it.

Senator DURBIN. And this is how our debate comes down. When you take the concept of minimization which basically says yes, keep us safe but don't sweep into your net innocent Americans who are doing things that are "constitutionally protected" in your own words.

I might also add that this reference, frequent reference here at the committee to the use of Grand Jury subpoenas, I hope you will acknowledge that the language that we are talking about here under 215 when it comes to gag orders for example, is substantially different than current language in the law when it comes to the use of Grand Jury subpoenas. Would you acknowledge that?

Mr. KRIS. I do, and as I said in response to Senator Feingold's questions, there are differences between ordinary criminal investigations and intelligence investigations.

I mean, I do think that it is a legitimate policy debate to have and we are having it in an orderly fashion.

Senator DURBIN. I would just like to close by saying I started off kind of with a negative view of librarians in my early life, but I want to salute them.

Mr. KRIS. You have come to admire them more?

Senator DURBIN. I have come to admire them more and salute them for the important role they play in this national debate. Thank you very much. Thank you.

Chairman LEAHY. Thank you. When it comes to librarians, Senator Durbin, I would mention that one of the formative parts of my

life was in the library at the age of four in the—Library in Mount Pilier, Vermont.

Ms. Holbrook, who was the librarian, and what she did to urge me to read. The library is much, much larger now and has a new wing partly paid for by some residuals from Batman movies. There is a long story behind that which I won't go into here.

Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Chairman. I wanted to ask you both about two issues. The roving wire tap, I understand the need for it. I have seen the nuisance that one has to go through to track a phone or track an individual over multiple phones and other investigations from my prosecutor days and obviously the 215 order has its purpose. I don't think at this point the discussion is about whether or not to continue any of these authorities. The question is what refinements might be necessary.

I am concerned as I think some of the other senators and witnesses have been about the question of the presumption that certain things are relevant. I ask first I guess, Mr. Kris, if you could tell me what effect a presumption has as a matter of kind of standard law.

Mr. KRIS. Right. Well, Senator, from your days as a U.S. attorney and as a lawyer, you know a presumption is just what it sounds like. It pushes you toward the finish line of establishing what you need to establish.

Senator WHITEHOUSE. But it has a particular effect, doesn't it? Doesn't it have the particular effect of shifting the burden of either production or persuasion in a particular matter?

Mr. KRIS. I mean, I think in an ex parte setting like this one as opposed to in a——

Senator WHITEHOUSE. Precisely my problem with it. If as a matter of Horn Book law the presumption has the legal effect of shifting the burden of persuasion or proof to another party and you are in an ex parte proceeding where there is no other party, I would submit to you that we are using the wrong language and the wrong tools to work through the problem that that is designed to solve.

Rather than continue to exist in a sort of fairyland in which a burden shifts to an empty chair and we all pretend to be satisfied with that set of procedures, we should maybe try to rethink how to do that in a more logical and sensible way that doesn't defeat what a presumption is all about in the first place.

I'm correct that there has never once been an adverse party that showed up in a 215 hearing. Not once.

Mr. KRIS. Not to my knowledge, no.

Senator WHITEHOUSE. And you would know.

Mr. KRIS. There is a vacuum process, but not at the front end. I guess a couple of points though in response. I think it is a fair question.

You are a very precise and careful technical lawyer to pick up on this. I guess two responses. The first is——

Senator WHITEHOUSE. One of many not unheard of. I mean, it isn't something I just invited. This is a pretty well known problem.

Mr. KRIS. I should just confine myself to answering the question, shouldn't I? The first is in order to take advantage of the presumption under 215, we have to show in the statement of facts that we

are submitting certain things, the three elements that Senator Feinstein outlined before.

So one point is just this presumption doesn't come free. You have to make a showing at the front end in order to trigger it. So if that showing is satisfactory as a policy matter, then the issue evaporates.

Also I think as a practical matter you could quibble with the use of presumption here along the lines you stated. Maybe it is more than just a quibble. But at the end of the day the fact remains we need to establish reasonable grounds to believe that the documents are relevant.

If we can trigger the presumption by establishing those facts, we are most of the way home and you're right, there is no opposing party to rebut. But the statute is still the same in terms of ultimately requiring a showing of relevance.

Senator WHITEHOUSE. The other question in my time remaining has to do with the Lone Wolf provision which as has been indicated, has never been used. There is another sort of logical difficulty in its application in that it is hard to imagine that the proof that an individual is an agent of a foreign power which is one of the prerequisites for the Lone Wolf provision would not also include proof that they are working with shall we say a foreign power in which case it is hard to imagine that you would need the Lone Wolf provision.

What is the difference between what is required to prove that somebody is an agent of a foreign power? Agency implies multiplicity. It is almost a legal impossibility to be acting purely alone and yet be the agent in the legal sense of that term of some other entity.

If you could walk me through that conundrum, I'd appreciate it.

Mr. KRIS. I'm going to come next time with a Horn Book. I think this one is genuinely a labeling concern. The way the statute was established in 1978, it defined two possible kinds of targets. Foreign powers and agents of foreign powers with the latter typically being an individual associated in one of the specified ways with the former. So Osama Bin Laden being an agent of Al Queda, Al Queda being the foreign power.

When Congress enacted the Lone Wolf provision, they said we are going to call this individual an agent of a foreign power because that is where it is going to fit in terms of the headings of the statute. But obviously the whole point——

Senator WHITEHOUSE. But he doesn't really have to be one?

Mr. KRIS. That's right. I mean, the whole point of the Lone Wolf provision is that there isn't a foreign power, there isn't an international terrorist group as there normally would be.

Senator WHITEHOUSE. And yet that remains a nominal requirement for the Lone Wolf authority, doesn't it?

Mr. KRIS. Well, I don't think it's a nominal requirement. This is what I mean when I say it is really just a labeling requirement. They are calling this person an agent of a foreign power and so that definition which is used throughout the statute is a convenient thing to hitch your wagon to here so that you don't have to re-write the entire statute all the way through. But I don't think it is meant

to fool anybody or that Congress misunderstood when they enacted it that there is some foreign power lurking behind this guy.

There may very well be, but whether there is and we just can't establish it or whether there is indeed no foreign power because he is a genuine free agent I think it is clear the statute is meant to cover that and they call him an agent of a foreign power because it fits in with the grammar of the rest of the statute.

Senator WHITEHOUSE. My time has expired.

Chairman LEAHY. Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much, Mr. Chairman, and thank you to both of you for being here. As I said during the confirmation hearing for Attorney General Holder, I support the extension of these three provisions. I think that they are important.

I first wanted to follow up on what Senator Whitehouse was talking about with the Lone Wolf provisions. Do you see given the fact that it hasn't been used, are there some changes that should be made to it to make it more usable?

Mr. KRIS. It is hard for me to imagine, I mean, there are a number of policy judgments involved in the Lone Wolf provision. For example, it does not apply to U.S. persons. It would be a major policy shift if you extended this thing to U.S. persons as opposed to non-U.S. persons.

Senator KLOBUCHAR. Agreed.

Mr. KRIS. And I'm not advocating one way or the other on that from where I sit today.

I think it is important to have this provision. The fact that we haven't used it yet doesn't mean that we won't use it or won't need it at some point in the future. As I said, I think in the letter that we sent on September 14th to Senator Leahy and in my testimony, in the age of the internet and decentralized Al Queda, I think there is the possibility of a person who is inspired by but not a member of an international terrorist group or the possibility of someone who is a member of a group but then breaks with the group for whatever reason. Perhaps it is not sufficiently radical for his tastes.

In either of those two situations, the person would be engaged in a national terrorism, wouldn't be any longer or ever a member of a group and would be I think someone who we would want to be able to cover. So I think we should reenact it and I don't, or reauthorize it. I guess I don't have specific ideas for changing it that I would advance on behalf of the administration.

Senator KLOBUCHAR. OK. Thank you. You started out with your testimony saying that you're willing to work with Congress on specific proposals and one of the reasons we have these sunsets is so we can see if there is some improvements or changes we can make.

But your testimony didn't address any possible changes. Should we take this to mean that the DOJ has not found any significant problems in either the structure or exercise of these authorities that would warrant modification?

Mr. KRIS. Well, I think what has actually happened is that Congress has seized the initiative here. Senator Leahy has dropped a bill, Senator Feingold and others as mentioned, and so what we are doing right now is we are looking hard at those bills and there are a lot of provisions in them, a very complicated area of law. We are

reviewing them aggressively and trying to figure out whether the provisions that are suggested there will work for us as is or perhaps with modifications.

So I think the dialog is joined because you have put several provisions on the table for us to look at and we are doing that.

Senator KLOBUCHAR. Senator Whitehouse had also said—through wire taps and sought authorization of wire taps on a state level, county attorney level, and so I know how complicated these minimization procedures are and what protections are in place.

Do you think that the protections that we have in place are sufficient to protect innocent Americans whose personal information might be caught in either a roving wire tap or Section 215?

Mr. KRIS. I think the existing law does protect very well and I think in part that is because of the diligence of the FISA court which pays very careful attention to the way these authorities are used.

That doesn't mean of course that they can't be improved. There is a lot of different ways to build these statutes and combine various elements and that is why we are open to working with you without condemning the existing law.

Senator KLOBUCHAR. And then Mr. Fine's testimony states that the FBI has said that the department has dropped the new minimization procedures for business records but these procedures haven't been issued.

When do you think these will be issued, and could you discuss how they might differ from the current minimization procedures?

Mr. KRIS. I am always reluctant to give a prediction about the timing of a deliverable, but it does seem to me that we are getting close. In terms of the content, I would be reluctant to discuss that in an open hearing.

Senator KLOBUCHAR. OK. In your review of the minimization procedures, did you see any problems that deserve our attention? Do you want to not discuss that either right now?

Mr. KRIS. Yes, I think I should defer getting into the possibly classified details of anything there.

Senator KLOBUCHAR. OK. On the Lone Wolf provision that we just talked about, and I will ask this as my last question. Do you believe there is any gaps in the definitions? I want to go back to that again, that we could change to make it more usable that wouldn't inhibit any intelligence gathering.

Mr. KRIS. We are really not seeking any expansions of the definitions of foreign power or agent of foreign power at this time.

Senator KLOBUCHAR. All right. Thank you very much, Mr. Kris.

Chairman LEAHY. Thank you. Mr. Kris, I made a note that many of us have had briefings on some of the aspects of the classified matters that you're talking about. We have several members of the, in both parties by tradition in the intelligence committee on the Judiciary Committee for that.

If you feel as you look over your answers there are things that you need to be answered in a classified version, we can arrange to have that provided for Senators and cleared staff. So if you feel that you are unable to give a full answer to Senator Klobuchar's question and anybody else and wish to follow up, please avail yourself of that and we will arrange it.

Senator Franken.

Senator FRANKEN. Thank you, Mr. Chairman. Mr. Fine, I am going to ask you a question soon.

Mr. FINE. Okay. I'm waiting for it.

Senator FRANKEN. First, Mr. Kris, I'm not a lawyer like all the, my colleagues here now nor a careful lawyer like you singled out. But I did some research and most Americans aren't lawyers.

So I've got a question on the roving wire tap thing and I think I understand why it is important because of the terrorists and other people we suspect of being terrorists use different phones, right?

Mr. KRIS. Yes.

Senator FRANKEN. Okay. And that's why it is there. But under the Patriot Act, the roving wire tap provision does not require law enforcement officials to identify the individual or the phone or the computer that will be tapped, is that right?

Mr. KRIS. No, I don't think so. The statute requires roving or not that the government identify, provide the identity if known or a description of the specific target.

Senator FRANKEN. A description of it, but not the actual name.

Mr. KRIS. Not always the name, but you have to say something about the specific target.

Senator FRANKEN. Okay. That is what brings me to this because they give you this when you get in the Senate. It is a constitution, and I was sworn to uphold it or support it anyway and protect it.

This is the Fourth Amendment. The right of the people to be secure in their persons houses, papers and effect against unreasonable searches and seizures should not be violated and no warrants shall issue but upon probable cause supported by oath or affirmation and particularly describing the place to be searched and the persons or things to be seized.

Now, it seems to me, that is pretty explicit language. I was wondering if you think that this is consistent with the Fourth Amendment.

Mr. KRIS. I do think it is and I kind of want to defer to that other third branch of government. The courts in looking at——

Senator FRANKEN. I know what they are. Go ahead, sir.

Mr. KRIS. The courts prior to FISA, prior to FISA every Court of Appeals to squarely consider the question had actually upheld warrantless foreign intelligence surveillance, that is without an advanced court order. The Supreme Court had declined to hold that a warrant was required in the so called Keith case for foreign intelligence surveillance. So I think you begin with that baseline.

FISA then by requiring advanced judicial approval goes above and beyond what the constitution requires for this kind of foreign intelligence surveillance. I do think there is an argument and probably a good argument that the language that I read to you before, that even if you cannot identify the particular target but that you describe the specific target that it would satisfy the particularity clause that you just cited.

Senator FRANKEN. Thank you. I want to get to Mr. Fine.

Mr. FINE. Thank you.

Senator FRANKEN. You're welcome. When the FBI wants documents for an investigation, it can either go to the FISA court or it can get one of these national security letters, right?

Mr. FINE. Right.

Senator FRANKEN. And for national security letters you don't need approval of the FISA court, right?

Mr. FINE. You don't need a court approval for a national security letter.

Senator FRANKEN. Okay. So I'm wondering what is to keep the FBI from always using the national security letter. So let me ask you, are national security letters now being used to get around higher requirements of the FISA courts for formal business records?

Mr. FINE. National security letters only apply to certain types of information from certain providers. So it can be used in those contexts. It cannot be used in other contexts.

So what limits it is the five statutes under which national security letters are authorized which specify very clearly where they can be used and where they can't be used. That is why, for example, the importance of Section 215 orders because there are certain types of records and things that can't be obtained by national security letters that have to be obtained by Section 215 orders.

Senator FRANKEN. I'm not sure that was, I didn't understand. Was that a yes or a no?

Mr. FINE. No, I don't think they are using it to get around the law.

Senator FRANKEN. Okay. Let me ask you, have they ever been used to get around?

Mr. FINE. I think they have improperly used them. I don't think it was intentional, that there were instances where we know we can't get these records but we are going to use them anyway. I think it was because of sloppiness, lack of training, lack of supervision, lack of knowledge, and those are the things that needed to be improved and rectified. That is what we pointed out in our report. I think the FBI has made some improvements in that area, but I think we need to still monitor it and oversee that.

Senator FRANKEN. Okay. That is just a concern of mine that, you know, if they can be misused and have been misused, that they will be misused in the future. That is a concern of mine.

If men were angels, there would be no need for government. I think that's Madison. You know, if angels were the government, we wouldn't, you know, need external controls. So I worry about the next administration might not be as trustworthy as this one or the last one.

Mr. FINE. That's why I believe there needs to be, as I stated in my statement, aggressive, important oversight mechanisms that don't rely on individuals that have controls on this so regardless of the administration there will be ways to verify and oversee and determine if they have been used properly or not. That is properly our role and partly other's role as well including national security and Congress for holding these important hearings.

Senator FRANKEN. Thank you. I have used my time.

Chairman LEAHY. Thank you. I will submit for the record a resolution to the Vermont Library Association a letter from the Con-

stitution Project as part of the Leahy/Cardin/Kaufman bill statement submitted to ACLU and others.

I was sort of thinking, I was pulling out some notes here as Senator Franken was asking this question. We have the FISA authority, and I direct this to you, Mr. Kris. We have the FISA authority to obtain tangible things such as library or medical business records.

Then we have the Title 18 Authority to issue national security letters. Now, you testified earlier and we have all agreed these can't be issued based solely on conduct protected by the First Amendment but the Inspector General found that in one case the FBI was twice denied tangible things ordered by the FISA court and the FISA court which normally grants these turned them down because they said the underlying conduct was protected by the First Amendment and there is no other basis in which to issue an order.

So the FBI then just turned around and issued a national security letter based on the exact same conduct protected by the First Amendment having been turned down by the court they went and did it administratively.

I think that is why you have a lot of Americans on the right and left who are worried about intrusive and unchecked government surveillance. We all want to be safe. We all want to catch criminals. That is not the issue.

The issue though is each one of us is our own privacy. The vast majority of Americans are law abiding Americans. If there is, the material is picked up, they go to data banks and then they can't get on an airplane, they can't get a job, they can't, the kids can't get a student loan, and you know all the horror stories.

We had a former longest serving member of this committee, the late Senator Ted Kennedy was eight or nine or ten times refused to go on one of the, an airplane or a flight he had been taking for 40 years back to Boston because he somehow is named on one of these lists.

So my question is, and I think this is what Senator Franken was saying too, what do we do to ensure this sort of thing isn't repeated? I mean, you talk about standards and whatnot. How do you ensure that these standards are followed?

I mean, I know you follow them. I know the Attorney General follows them. I know the Director will follow them. Well, how do we make sure the agents out in the field follow them?

Mr. KRIS. Senator, it is an excellent question and I think a very trenchant one. I mean, I think there is a variety of different interlocking methods that can be used to protect against misuse or abuse.

The first is writing the law, setting the standards at a certain level and that is something you can do through amending the statute. The next is within the executive branch through training, oversight by Mr. Fine's office, in some cases my office, the National Security Division does oversight of the FBI.

There are electronic systems, for example, for national security letters. The FBI developed an electronic subsystem that essentially ensures that all of the requirements are met before a letter can be issued so we can develop internal systems.

They have an Office of Integrity and Compliance as Mr. Fine talked about that does oversight, and obviously congressional oversight whether fueled by a sunset provision or just more generally about the use of the authorities can provide an effective check, and in some cases, the courts. So a variety of different methods.

Chairman LEAHY. Let me use one concrete. In the 2006 USA Patriot Act Reauthorization, we required, and I helped write this, the Attorney General to adopt procedures to minimize retention and improper dissemination of private information that was obtained by Section 215.

Going back to what I was referring to earlier about all the material that is in data banks floating around there in every one of us. Again, I know most Vermonters are somewhat concerned about their privacy but I think they are in every state.

Minimization procedures are supposed to protect the constitutional rights of all of us. But Mr. Fine, you found in your March 2008 report these safeguards that everybody agreed on, Republicans, Democrats, everybody else, minimization. They were never put in place. The Attorney General simply recycled the FBI's national security investigation guidelines, adopted those as the interim minimization procedures you found were woefully inadequate.

They didn't follow the statute. It is one thing to talk about oversight and all that and the reauthorization, but the statute is not followed and it is a concern. Now we have a new Attorney General who followed up on your recommendation that specific minimization procedures be developed and adopted. Do we have those procedures now?

Mr. FINE. No, they have not been issued. As I pointed out in my statement, they adopted these interim procedures that were not specific that they believe that comply with the statute, but we believe that there ought to be those specific minimization procedures as contemplated by the Patriot Reauthorization Act that do apply specifically to Section 215 orders and they have been in draft, they have been in draft for a long time. We think they ought to be considered, finalized and issued.

Chairman LEAHY. I will, my time has expired. I will follow up more on this. I just wanted to get the information. But if it's not something you need, I want to get it out of the data banks. I don't want it to cloud over me when I get on an airplane or when my constituents do or when they apply for a job or whatever else it might be.

I won't go into discussions of George Orwell and everything else, but these things can be frightening. One of the great things about this country is we have always said we'd balance. Senator Sessions? I don't want material in there on Senator Sessions that shouldn't be there.

Senator SESSIONS. Well, 1984 came and went and the communists didn't get us. I'm glad to have been on the right side of that battle.

The idea of keeping, maintaining confidentiality of an investigation, Mr. Kris, can be exceedingly important in a national security matter, a terrorism matter. From what I see in the paper, and I don't have any inside information, I believe the New York Times

reported again today that in this case, arrests have been made in the Afghan case, that the New York police wanted to inquire of an Iman about the individual, or an individual and asked him not to reveal that but asked him for information about this person as they tried to figure out what may have been happening.

What I understand from the reports is that he went straight and reported it to one of the members connected to this individual and that may have been, caused the entire investigation to be altered and made perhaps more difficult to identify people that are involved in a plot to attack and kill American citizens.

Isn't that a legitimate concern and can't we do that based on historic settled principles of American constitutional law?

Mr. KRIS. It is a very grave concern when information that compromises an investigation is leaked for the reasons that you stated. It can have very profound effects on our ability to investigate matters and I think existing law in the confidentiality requirements and the secrecy requirements exist precisely for that reason, in order to protect the secrecy of the intelligence investigations because if they are made public, they can be compromised.

Senator SESSIONS. And it hasn't always been recognized that there is a huge difference between surveillance and investigations of foreign powers, espionage and counter espionage than investigations of American citizens.

Mr. KRIS. There has historically been recognized in law and in policy, yes, a distinction between security threats based abroad, that is foreign security threats on the one hand, domestic security threats, domestic terrorism and ordinary law enforcement on the other.

Senator SESSIONS. I think Senator Franken's comments about the Fourth Amendment, the right of the people to be secure in their houses, papers, effects against unreasonable searches and seizures.

So we have set up a system by which you have to go to a Federal judge in a Federal case and submit extensive evidence to justify a search. But I would also want to emphasize to my colleagues and Senator Franken, records held in a bank are not your records, they are the bank's records.

In a motel sign-in sheet that could be decisive in a case is not the person who registered's records, it is the motel's record. That is why the courts have always recognized that it does not violate this court.

Now, when I was watching Senator Franken I talked about Dragnet, Joe Friday and company. They used to go out to the motel and get the records to see if old Billy checked in. And they would give it to them. Now because of the laws and lawyers, banks and everybody often demand subpoena or some sort of official document before they will turn it over because they don't want to be sued by somebody and have to defend the case whether they win or lose.

But the principles are pretty much the same here. You have a diminished expectation of privacy and records held by independent third parties. Isn't that right?

Mr. KRIS. I mean, I certainly agree under the Miller case in particular that you do have a diminished expectation of privacy in such materials and in some cases Congress has seen fit to enact

protections by statute by such material. For example, ECBA is a major example.

Senator SESSIONS. Now, with regard to these nondisclosure orders, which as a former prosecutor, these investigated drug organizations, one of the most delicate, important matters is when you start making arrests.

If you arrest some low level guy the first time you have a bit of evidence, the rest of them scatter. They flee, they cover their tracks. They disappear. That is even more critical in a terrorism investigation to me.

But isn't it true that it takes the direction of the FBI or his high level designee to justify, certify that a non-disclosure order is needed, and isn't that one thing that the Patriot Act did to ensure that it is not done willy nilly without some thought and oversight?

Mr. KRIS. Certainly with respect to Section 215 a relatively high ranking person makes a submission and then the court grants an order. With respect to NSLs, there is no court order and the Doe decision from the Second Circuit found First Amendment difficulties with that and suggested a so-called reciprocal notice procedure that the FBI has adopted which I think responds to that concern.

Senator SESSIONS. Well, as a Federal prosecutor, I remember distinctly that we would issue subpoenas in FBI cases. The Grand Jury was not advised until later. No Federal judge was given any notice of it and the FBI went out and served it.

They were always irritated as the United States attorney, Mr. Whitehouse, my colleague here, will know that the DEA could get a subpoena to go out to the telephone company or the bank and get records without asking the U.S. attorney's permission.

It is not a historic alteration of American criminal jurisprudence to have a national security letter in my opinion, and it is in an area that is very, very, very important to our safety. Thank you.

Senator WHITEHOUSE. Thank you, Senator Sessions. A question for Mr. Fine. Your report when it first came out on the national security letters——

Senator SESSIONS. Mr. Chairman, can I interrupt you just to say that my Republican colleagues, at least three are in the Finance Committee trying to do the health care thing. They would have been here otherwise. I wanted to state that for the record. It is a matter I think all of us take seriously.

Senator WHITEHOUSE. It is for the record that we're trying to do the health care thing?

Senator SESSIONS. They are trying to do a good health care bill.

Senator WHITEHOUSE. When the report came out, it dealt very heavily with operational issues, failures out in the field of people to adhere to the different regulations and statutory requirements that had been put in place for the issuance of those national security letters.

One of the points that I raised with the Director at the time was that it also showed a very significant organization and management failure. These national security letters were issued pursuant to statutory authority that a lot of people in this building had real reservations about. Republicans and Democrats alike, and set a lot of markers saying all right, we will give you this, we will trust you, but here is what you have got to do.

In terms of the credibility of the Federal Bureau of Investigation as an institution in this building, one would have thought that there would have been somebody at the very highest level reporting to the Director saying wow, we got this new authority under very strict requirements and kind of on trust in the confidence that we would follow those rules. Therefore, to us as an institution it is really important that we follow those.

I, as that imaginary person, am really, it is my job to make sure of this so that when we come back for other authorities later on, we don't get into the cry wolf problem of hey, we trusted you last time, you completely blew it and now you don't have the same trust with us any longer.

That struck me as being a significant institutional gap that the FBI wouldn't have somebody in their leadership whose job it was to basically protect that flank of theirs from their own junior folks' lack of adherence to these different things.

In your review of this on an onging basis, are you comfortable not only that at an operational level the FBI has improved its adherence to the various protocols for national security letters, but at the management level they have a sensitivity to the importance of adhering to whatever the trust is that Congress has given them and that there is more management oversight of all compliance and adherence and regulatory measures than this displayed?

Mr. FINE. Yes. I think that as a result of our report in March 2007 the FBI was—by it and you are absolutely right, there was an institutional failure.

They received these very important and vital authorities, but they did not take measures to ensure that they would be used properly and they just assumed that it would be used properly.

When we came out with our report, it was very eye opening for them and I do remember even at the time Director Muller stating that clearly, stating he took responsibility in stating to be honest that he was at fault for not putting in the measures to ensure that these authorities that they are given are used properly.

You cannot simply put out a memo and then think it is all going to be followed in the 56 field offices of the FBI. You have to make sure that they are trained constantly, that they are supervised, that they are overseen and that they are monitored and audited. I think they have made strides in that direction. They made significant progress.

I mentioned the Office of Integrity compliance, they did inspection division reviews, we have national security division reviews, but I don't think being an Inspector General that you can simply say that is going to solve all the problems and you can stop doing it and we can rest assured. You have to continually be vigilant on it and we are going to do a review of the Office of Integrity Compliance.

Are they fulfilling their stated mission? Are they having an impact? Or was this simply another office that was created that is not being effective? We don't know that for sure. We are going to determine that. But that is what the FBI also has to do on an ongoing basis rather than simply assuming that the measures they have implemented are going to be effective.

Senator WHITEHOUSE. And it is your observation that as an institutional wake up call, this incident did in fact have that effect?

Mr. FINE. I think it did. I think it was a very, very significant eye opening experience for them when they saw how significant our findings were and that they hadn't found them, that we found them and exposed them and they were not happy about that.

Senator WHITEHOUSE. Senator Franken.

Senator FRANKEN. Thank you, Mr. Chair. Senator Whitehouse did actually follow up with what I wanted to follow up with. I just want to make it clear to Mr. Kris that what I was talking about was the roving wire taps and when Senator Sessions referred to it, I think it was Section 215. So those are very different issues.

I understand that hotel records aren't the record of the person, but when you are doing a roving wire tap and you're not telling the FISA judge either the identity of the person or exactly where you want to tap them, that just caused me concern on the reading of the amendment in the constitution.

Mr. KRIS. Yes. No, I understood absolutely the difference there.

Senator FRANKEN. Okay.

Mr. KRIS. You have raised what I consider to be a particularity clause in effect a problem that the warrant or the order under FISA is not sufficiently precise and particular in specifying exactly what is to be done.

I tried to give you an answer to that question, but I think we——

Senator FRANKEN. Okay. I just wanted to make it clear that, because in response to Senator Sessions, I don't think you made the distinction or made it clear that there was a distinction between what I was asking and what Senator Sessions was discussing.

Mr. KRIS. Yes, sir. There is a very significant distinction between Section 215 and FISA collection. I mean, what we are talking about in a roving wire tap or an ordinary wire tap is the collection of content of communications. That enjoys much greater constitutional protection than do say business records that are held by a third party absolutely.

Senator FRANKEN. Okay. I just wanted to make that clear. Thank you. No further questions.

Senator WHITEHOUSE. All right. I thank the witnesses very much for their testimony. We will take a minute or so to reset the room for the second panel and then we will proceed with the hearing.

[Off the record at 11:48 a.m.]

[On the record at 11:51 a.m.]

PANEL II

Senator WHITEHOUSE. The hearing will come back to order. Why don't I begin by asking the various witnesses to stand and we can get them sworn.

Do you affirm that the testimony you're about to give before the committee will be the truth, the whole truth and nothing but the truth so help you God?

Group Answer. I do.

Senator WHITEHOUSE. Please be seated. We have a particularly distinguished panel here this morning and I would like to welcome all three witnesses. I am delighted that they are here.

I think what I will do is make all three introductions right away and then we will proceed across the panel beginning with Ms. Spaulding.

Suzanne Spaulding is a Principal with Bingham Consulting Group and of counsel to Bingham McCutchin in Washington, DC. She has spent over 20 years handling national security issues for Congress and the Executive Branch, including serving as Assistant General Counsel out at the CIA, Minority Staff Director for the House of Permanent Select Committee on Intelligence, General Counsel for the Senate Select Committee on Intelligence and as Legislative Director to Senator Arlen Specter.

Kenneth Wainstein is currently a partner at O'Melveny & Myers where he works in the white collar crime group. Mr. Wainstein is the first Assistant Attorney General for National Security serving in the Bush Administration. He also served as Homeland Security Advisor to President George W. Bush and as a United States Attorney for the District of Columbia.

Ms. Lisa Graves is the Executive Director of the Center for Media and Democracy at the University of Wisconsin. She has served as a Senior Advisor in all three branches of the Federal Government and is a leading strategist on civil liberties and constitutional protections.

She served as Chief Nominations Counsel to Senator Leahy from 2002 until 2005. We welcome you back to the Judiciary Committee. We welcome all of the witnesses. We are honored to have you with us. Those of you who I have had the experience of their work in public service, I am particularly grateful to have you back here today. Thank you for your service.

Suzanne Spaulding.

STATEMENT OF SUZANNE E. SPAULDING PRINCIPAL, BINGHAM CONSULTING GROUP, WASHINGTON, DC

Ms. SPAULDING. Thank you, Acting Chairman Whitehouse, Ranking Member Sessions and members of the committee. Thank you for your invitation to participate in today's hearing on Ensuring Liberty and Security.

Earlier this month we marked another anniversary of the attacks of September 11th. In the 8 years since that indelible manifestation of the terrorist threat, we have come to better understand that respect for the constitution and the rule of law are a source of strength and can be a powerful antidote to the twisted lure of the terrorists.

In fact, after spending almost 20 years working national security and terrorism issues for the government, I am convinced that this approach is essential to defeating the terrorist threat.

Given this national security imperative, Congress should use this opportunity to examine more broadly ways to improve our overall domestic intelligence framework, including a comprehensive review of FISA, national security letters, attorney general guidelines and applicable criminal investigative authorities and I would encourage the administration to do the same.

This morning, however, I will focus my remarks on the sunsetting provisions that are the focus of this hearing. Sections 215 and 206 both have corollaries in the criminal code. Ultimately,

however, important safeguards were lost in their translation into the intelligence context.

Section 206, for example, was intended to make available an intelligence surveillance, the roving wire tap authority that criminal investigators have. This was an essential update. However, there are specific safeguards in criminal Title 3 provision that were not carried over to FISA, requirements that provided significant safeguards designed to protect Fourth Amendment rights of innocent people.

Their absence in Section 215 increases the likelihood of mistakes and the possibility of misuse. In addition, in the criminal context where the focus is on successful prosecution, exclusionary rules serve as an essential deterrent against abuse, one that is largely absent in intelligence operations where prosecution may not be the primary goal.

This highlights the care that must be taken when importing criminal authorities into the intelligence context. And why it may be necessary to include more rigorous standards and other safeguards. I have suggested in my written testimony some ways to address these concerns.

Similarly, Section 215 governing orders for tangible things attempted to mimic the use of Grand Jury or administrative subpoenas in the criminal context. However, criminal subpoenas require some criminal nexus, FISA's 215 does not.

Moreover, the Patriot Act amendments broaden this Authority well beyond business records to allow these orders to be issued to obtain any tangible thing from any person. This could include an order compelling you to hand over your personal notes, your daughter's diary or your computer. Things to which the Fourth Amendment clearly applies.

Again, in my written testimony I have tried to suggest ways to tighten the safeguards without impairing the national security value of this provision. In the interest of time, however, I will move to the Lone Wolf provision.

Four years ago I urged Congress to let the Lone Wolf provision sunset and I reiterate that plea today. The administration admits that Lone Wolf authority has never been used but pleads for its continuation just in case.

The problem is that this unnecessary provision comes at a significant cost of undermining the policy and constitutional justification for the entire FISA statute, a statute that is an extremely important tool for intelligence investigations.

Legislative history, court cases before and after the enactment of FISA including two cases from the FISA court itself make clear that this extraordinary departure from Fourth Amendment standards is justified only by the unique complications and secrecy requirements inherent in investigating foreign powers and their agents.

Unfortunately instead of repealing or fixing Lone Wolf, Congress expanded it by adding a person engaged in proliferation. There is no requirement that this activity be unlawful or that the person know that they are contributing to proliferation.

So someone who is involved in completely legal sales, for example, of dual use goods, unbeknownst to her that are being sold to

a front company could be considered to be engaged in proliferation and have all of her phone conversations and emails intercepted and her home secretly searched by the United States government.

As a former legal advisor to the intelligence community's nonproliferation center and executive director of a congressionally mandated weapons of mass destruction commission, I fully understand the imperative to stop the spread of these dangerous technologies.

However, there are many tools available to investigate these activities without permitting the most intrusive and secretive techniques to be used against people unwittingly involved in legal activity.

In conclusion, let me commend the committee for its commitment to ensuring that the government has all the appropriate and necessary tools at its disposal in this vitally important effort to counter today's threats and that these authorities are crafted and implemented in a way that meets our strategic goals as well as our technical needs.

With the new administration that provokes less fear of the misuse of authority, it may be tempting to be less insistent upon statutory safeguards. On the contrary, this is precisely the time to seize the opportunity to work with the administration to institutionalize appropriate safeguards in ways that will mitigate the prospect for abuse by future administrations or by this administration in the aftermath of an event. Thank you.

Senator WHITEHOUSE. Thank you very much, Ms. Spaulding.

Mr. Wainstein, welcome back to the committee. Please proceed.

STATEMENT OF KENNETH L. WAINSTEIN PARTNER, O'MELVENY & MYERS, LLP, WASHINGTON, DC

Mr. WAINSTEIN. Thank you very much, Chairman Whitehouse. It is very good to be back here again.

Senator WHITEHOUSE. Good to have you back.

Mr. WAINSTEIN. Chairman Whitehouse, Ranking Member Sessions, members of the committee, thank you very much for holding this important hearing and for soliciting our views about the USA Patriot Act.

Today I want to discuss the three sunsetting provisions and the reasons why I believe they should all be reauthorized. As you well know, the Patriot Act was passed in late October, 2001 within a mere 45 days after the 9/11 attacks. Four years later in 2005, Congress in its enduring credit undertook a lengthy process of carefully scrutinizing each and every provision of the Patriot Act, a process that results in the Reauthorizaton Act that provided significant new safeguards for many of the original provisions.

We are now at a point where the authorities and the Patriot Act are woven into the fabric of our counterterrorism operations and have become a critical part of our defenses against what President Obama has aptly described as Al Queda's "far reaching network of violence and hatred."

This is particularly true of the three provisions that are subject to reauthorization this year. First, the roving wiretap authority. First, this provision allows agents to maintain continuous surveillance as a target moves from one telephone or communication de-

vice to another which is standard tradecraft for many surveillance conscious spies and terrorists.

This is a critical investigative tool and it is one that criminal investigators pursuing drug traffickers know their regular criminals have been able to use for years.

It is especially critical nowadays given the proliferation of inexpensive cell phones, calling cards and other innovations that make it easy to dodge surveillance by rotating communication devices.

While some have raised privacy concerns about this authority, the reality is it has a number of safeguards built into it to make sure that it is used appropriately. For example, it is specifically limited to those situations where the government can show to the FISA court that the target is swapping cell phones or otherwise thwarting the government's surveillance efforts and it requires the government to keep the FISA court fully apprised with detailed reports whenever they move their surveillance from one communication device to another.

Given the narrow application of the statute, given the FISA court's oversight of the roving surveillance and given the absolute imperative of being able to maintain uninterrupted surveillance on terrorists and spies who are in our midst, there is no question in my mind that the roving wiretap authority should be reauthorized.

Now, on to Section 215. Section 215 authorizes agents to get a FISA court order that will compel businesses to produce the same kind of records that law enforcement officers and prosecutors have always been able to obtain to grand jury subpoenas.

Prior to the enactment of Section 215, our national security personnel were hamstrung in their effort to obtain business records because the operative statute at the time limited those orders only to certain types of businesses and required a higher evidentiary standard than grand jury subpoenas did.

Section 215 addressed these weaknesses by allowing these orders to be used to get records from any businesses or any entities and by squaring the evidentiary standard with the traditional relevant standard used for grand jury subpoenas.

At the same time, Congress built in a number of safeguards that protect against misuse and in fact make Section 215 significantly more protective of the civil liberties than the grand jury subpoenas that are issued by the hundreds or thousands by criminal prosecutors around the country every day.

For example, as Ranking member Sessions pointed out earlier, unlike grand jury subpoenas that a prosecutor can issue or his or her own, a 215 order must be approved by a Federal judge on the FISA court. Unlike the subpoena authority, Section 215 also does several other things.

It specifically bars issuance of an order if the underlying investigation is focused solely on First Amendment activities. It requires regular and comprehensive reporting to Congress and it imposes a higher standard when the government seeking library records or other sensitive records.

With these safeguards in place, there is simply no reason in my mind that we should be returning to the days when it was easier for a prosecutor to get records in a simple assault case than it was for national security investigators to obtain records that might help

defend our country against a terrorist attack. Section 215 should be reauthorized.

Last, the Lone Wolf provision. This provision allows the government to conduct FISA surveillance on non-US persons who engage in international terrorism without having to demonstrate that that person is affiliated with a particular terrorist organization.

When FISA was originally passed back in 1978, it contemplated terrorist target of FISA surveillance was the agent of an organized terrorist group kind of like the Red Brigades, the kind of target that easily fit within the statutory definition of an agent of foreign power.

Today we face adversaries that range from loosely knit terrorist networks to self-radicalized foreign terrorists who may not be part of a particular terrorist group but who are nonetheless just as committed to pursuing the violent objectives of international terrorism.

As a result, there is a risk today that we will encounter a Lone Wolf foreign terrorist who cannot be identified with a known terrorist group and therefore would not qualify for FISA coverage under the original statute.

Congress solved this problem by passing the Lone Wolf provision. It allows for FISA surveillance based on a showing that the target is involved in international terrorism regardless of affiliation.

Although as the government reported we have not yet used the Lone Wolf provision, the threat posed by foreign terrorists, no matter what their affiliation, is more than ample justification for keeping this authority available for the day that the government might need it.

Thank you once again for inviting me here today. I am grateful for the opportunity to discuss the sunsetting Patriot Act provisions and to lay out my reasons why I firmly believe that they should all be reauthorized this year. I look forward to answering any questions you might have. Thank you.

Senator WHITEHOUSE. Thank you, Mr. Wainstein.

Ms. Graves.

STATEMENT OF LISA GRAVES, EXECUTIVE DIRECTOR, CENTER FOR MEDIA & DEMOCRACY, WASHINGTON, DC

Ms. GRAVES. Senator Whitehouse, Chairman Leahy who is not here, but who I was hoping to have the chance to address, Ranking Member Sessions and the members of the judiciary committee, I am very pleased to be here and I really appreciate the invitation.

I have a full statement for the record but I was hoping today for these opening remarks to focus on some of the things that have come up today in the conversation.

Before I begin, I do want to say that I am pleased to endorse the legislation sponsored by Senator Leahy and Senator Cardin and Senator Kaufman, the Patriot Sunset Extension Act. I think it is an important down payment on restoring civil liberties.

I am hoping that other improvements will be made. I would also like to endorse S. 1686 which is Senator Feingold's Justice Act. I think it is a comprehensive approach to some of the problems that have arisen over the last 7 years and I think that bill which is proposed by Senator Feingold and Senator Durbin is an important, has an important array of provisions to restore civil liberties.

VerDate Nov 24 2008 14:15 Apr 06, 2010 Jkt 055610 PO 00000 Frm 00040 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\55610.TXT SJUD1 PsN: CMORC

I want to focus my testimony today on Section 215 of the national security letters. But before I do that, I want to touch briefly on Section 206 and the particularity requirement issue.

I would only say that it is a bit difficult to focus on what the rules should be for roving wire taps in this context when we haven't had the needed reforms to the broader Foreign Intelligence Surveillance Act amendment Act, the FISA amendment Act that was pushed through last year.

What we have is a circumstance in which an enormous array of communications involving Americans, particularly international communications, telephone communications and internet communications are now accessible through blanket orders or broad orders without individualized particularity that are being approved by the FISA court.

So on the one hand we have an enormous array of information about American content spoken and written by Americans that is being obtained through the FISA Amendments Act powers. On the other hand we have this roving wire tap authority that exists and happens domestically that is distinct and yet to me not the biggest issue compared with what we have in terms of the broad authorities under the FISA Amendments Act. But I will save the rest of that for another day.

Today I want to focus on Section 215, the issue of business records, the issue of tangible things and national security letters.

So a lot of the conversation today focused on this presumption issue for Section 215 orders and whether something is relevant. But what the law now requires is merely that the government say that the records pertain to, that's the relevance test, do these record pertain to a particular person and that particular person can be someone who has contact with a suspected terrorist or someone who is under surveillance.

So mere contact is a very low standard. There are 100 people in this room. There may be 1,000 people you have contact with every year, probably a lot more than that. The government doesn't have to show any particular suspicious activity. Based on showing mere contact, they can have access to any tangible thing about you.

So relevant to what? Relevant to merely a person and that person doesn't have to be someone who is a suspected terrorist. In fact, what the Justice Department said in a report in 2006 was that the Patriot Act authorized the FBI to collect, and this is for national security letters which is basically the same standard, for national security letters the FBI is authorized to collect information such as telephone records, internet usage, credit and banking information on persons who are not subject to FBI investigations. This is according to the Justice Department.

This means that the FBI and other law enforcement and intelligence community agencies with access to FBI data bases is able to review and store information about American citizens and others in the United States who are not subjects of FBI counter intelligence investigations and about whom the FBI has no individualized suspicion of illegal activity.

That is why this issue matters so much. The 215 orders cover any tangible thing. The national security letters cover anything held by a bank, a credit card company, an insurance company, a

pawn broker, a real estate closing service, the United States postal service and a casino among other authorities.

So these aren't just narrow authorities that relate particularly to internet service providers and banks. They are broad authorities in the national security letter powers.

The ISP authority that came up in the context of the questions for about the library, what happened there is the FBI construed the library to be an internet service provider. If a library can be an internet service provider, then anyone can be an internet service provider. Any Senate office, any business that maintains an internet service would be basically accessible through these authorities. That is why they are so broad. That is why they need further containment and that's why the improvements that have been proposed by Senator Feingold and by Senator Leahy are so important.

These powers go to the heart of what the power should be for the government vis-a-vis the citizens of the United States and we know that these documents, the documents that are obtained through these powers are being put into FBI data bases. The FBI data base, the investigative data warehouse now has almost 1 billion records in it.

The Inspector General Glenn Fine said that the national security letter powers were used to clear cases, to clear people and close cases. But the FBI has said that even if you are cleared or your case is closed, those records will be maintained basically forever.

That is why your inquiry is so important and that's why I'm pleased to be here today to talk about the needed reforms for the Patriot Act authority that were expanded in 2001.

Senator WHITEHOUSE. Thank you, Ms. Graves. I will call on our distinguished ranking member first and then Senator Feingold and then I will wrap up unless other Senators appear. But first the distinguished ranking member.

Senator SESSIONS. Thank you. Mr. Wainstein, if records are obtained by the FBI as part of a terrorist investigation, how are they secured? Are they available to anybody that wants to walk in and look at them? Or are they kept in a secure circumstance regardless of what is normal criminal case or terrorist case?

Mr. WAINSTEIN. Well, sir, as you know in the criminal context there are procedures in place and have been since—to make sure that records that are secured by Grant Jury subpoena are kept confidential because there are rules governing any material that is collected in the course of the grand jury.

Senator SESSIONS. It's a criminal offense to reveal a grand jury document.

Mr. WAINSTEIN. Yes, sir, absolutely. Those procedures are even more strict on the national security side where you have classified information potentially and also national security information which is even more sensitive in some ways.

Senator SESSIONS. Ms. Spaulding, you signed a letter back in '05 to reauthorize the Patriot Act. Fundamentally you support it. Have you changed your view about the Lone Wolf issue?

Ms. SPAULDING. Senator, I have always been opposed to the Lone Wolf provision and I think what you are referring to is a letter by a bipartisan working group that states very clearly at the outset

VerDate Nov 24 2008 14:15 Apr 06, 2010 Jkt 055610 PO 00000 Frm 00042 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\55610.TXT SJUD1 PsN: CMORC

that what we were attempting to do was come together on a compromised package, overall package, and that it did not mean that all of the signatories agreed with each and every recommendation.

Senator SESSIONS. I understand. But in fact you concluded at the time it was worth passing even though you might have had a disagreement about that part?

Ms. SPAULDING. Well, I concluded at that time along with the other members of that group that the overall provisions of the Patriot Act had implemented some important updates and should be reauthorized with some changes as we recommended. I have always been opposed and continue to be opposed to the Lone Wolf provision.

Senator SESSIONS. I don't think that letter you wrote said it had to be taken out. But regardless, on the telephone you indicated that on the 215 your telephone conversations could be intercepted, is that correct?

Ms. SPAULDING. No, Senator. I think I said your personal notes, your daughter's diary and your computer, all of which are tangible things susceptible to a 215 order.

Senator SESSIONS. Well, if your daughter is connected to a terrorist organization, maybe that is important. I don't think the FBI is out just gratuitously wanting to peruse people's diaries. That's the only thing I would say here.

With regard to the 215, you say it could take your personal records. You cannot under 215, can you, take somebody's records that you own in your home or on your possession.

Ms. SPAULDING. There is nothing in the statute that would prohibit that. The Section 215 allows the government to compel anyone to produce any tangible thing.

Senator SESSIONS. So you think it can replace a search warrant?

Ms. SPAULDING. According to the plain terms of the statute, it does not have to be directed to a business or an entity. It can be directed to any person to compel any tangible thing.

Senator SESSIONS. Mr. Wainstein, can you utilize a 215 request to obtain a target's personal records in his desk drawer in his home?

Mr. WAINSTEIN. You raise a very good question, sir. I think the analysis is the same as on the criminal side. You know, the person would have certain privileges to invoke, so there is a mechanism for challenging a 215 order before the FISA court.

One of the bases for that challenge could be I have got a Fifth Amendment right not to disclose the items that are sought.

Senator SESSIONS. So on the 215 it is akin, I mean, it is, you go to the court first before you can execute it, unlike the national security letter which you can execute administratively essentially?

Mr. WAINSTEIN. Yes, sir. And as you pointed out, like any administrative subpoena, and there are I think 300 different types of administrative subpoenas out there for various civil and criminal kinds of enforcement.

In none of those situations does the agency have to go to the court. Then as we had both pointed out, the prosecutor doesn't need to go to the court before issuing a grand jury subpoena in a regular criminal context.

Senator SESSIONS. Do you say that there is an intellectual problem let me say with defining an entity at war with the United States, the Lone Wolf thing, as a single person as opposed to a multiplicity? Intellectually can't an individual be at war with the United States just as well as a group of people?

Mr. WAINSTEIN. Well, I think actually sort of stepping back and looking at taking it out of the context of, the terminology of a statute, looking at the purpose of the Lone Wolf provision, it is exactly that. There could be a person out there who is maybe working with international elements and is inspired by international terrorists, terrorist groups but we cannot hook that person to a particular group.

He could be just as dangerous and just as devastating to America and Americans as somebody who is a card carrying member of Al Queda.

Senator SESSIONS. The thing about these contacts and these records that might be issued to this or that bank or telephone company, the reality is that the person may be perfectly innocent but they may be in contact with a terrorist.

Just the fact that they have contact can be proof of something or prove they were in town, prove they were making communications, proving that they were furthering their agenda. Maybe it was to rent a U-haul truck to carry explosives in. Those kinds of things can be just critical to an investigation.

I think we struck the right balance. I think there is a lot of controls and limits and reviews over this. Senator Whitehouse, I think that Senator Leahy and others, we went through this weeks and weeks and it was not rushed through. It was a number of months of intense effort.

Senator Feingold held our feet to the fire time and time again on issues that he felt were important and won a number of battles and lost some. I think it was not just thrown together as a blind reaction to a terrorist attack. We did not just ignore our constitutional principles and traditional law enforcement principles. Thank you.

Senator WHITEHOUSE. Thank you, Senator Sessions.

Senator Feingold.

Senator FEINGOLD. Thank you, Mr. Chairman. The Senator from Alabama, I really enjoy working with him, but I wish I remembered those victories. I don't recall them, but it was an excellent experience trying to achieve them.

I want to thank this panel very much. Ms. Spaulding, you argued that the so called Lone Wolf authority undermines the policy and constitutional justification of FISA and the Congress allowed to sunset and I know Senator Sessions was talking to you a little bit about that.

As you know, the Justice Department argues that the authority should be reauthorized even though it has never been used. Can you explain why the connection to a foreign power is so important to FISA's constitutionality?

Ms. SPAULDING. The reference to the foreign power and agent of foreign power as underlined the justification for FISA comes out of a Supreme Court case in which they were looking at a domestic na-

tional security case and decided that the traditional Fourth Amendment warrant requirements would still apply there.

In a footnote they said that they were not ruling on cases that involved foreign powers or agents of foreign powers because of the unique complications and requirements inherent in those kinds of investigations.

Clearly one of the key aspects of FISA that is beneficial in intelligence investigations is the secrecy. It is also a source of concern as you noted and as we have discussed this morning. But the secrecy with respect to FISA electronic surveillance versus the ability to use a Title 3 criminal wiretap which is always an option for a Lone Wolf or anyone else, it really goes to the sensitivity of the information in the application for an electronic surveillance under FISA and the sensitivity really derives from the information you would put in that application, tagging this person to a group.

It is the information that you have in that application with regard to the broader activities of a terrorist group that make it so sensitive and different from a Title 3 criminal application with respect to an individual.

That sensitivity simply isn't as pronounced when you are going after a Lone Wolf, a single individual that you are not tying to a group. Your application is going to contain——

Senator FEINGOLD. So is the option of a criminal wire tap order an adequate alternative in the Lone Wolf situation?

Ms. SPAULDING. I think a Title 3 wiretap application ought to be sufficient. I think if the government can make the compelling case that if they determine there is actually attachment to a group, perhaps Congress would want to consider allowing a transfer then from a Title 3 to a FISA with the secrecy. I think there are ways to work through that but I think that Title 3 wire tap for these True Lone Wolf ought to be sufficient.

Senator FEINGOLD. Ms. Spaulding, last week I asked the FBI Director Muller if the FBI had made any changes to the way it handles the gag orders associated with Section 215 orders as a result of the second circuit decision ruling that the gag orders associated with the national security letters violate the First Amendment. The section 215 issue was of course not directly addressed by the court which was considering NSLs, but the court's opinion certainly seems to have some implications in the same context.

Yet Director Muller said the FBI has not made any changes to the way it handles 215 gag orders. What is your view on the applicability of the court's decision to gag orders under Section 215 and does the FBI's position suggest that legislative changes are needed?

Ms. Graves.

Ms. GRAVES. Thank you, Senator Feingold. I would say that clearly the language in the second circuit's decision is applicable. It is relevant to how these matters should be addressed by the government.

To take a very narrow view of that decision which was in the national security letter case and say because it deals with Section 505 of the Patriot Act, even though the gag terms are similar if not substantially the same, it shouldn't be applied to Section 215 gag order is the wrong approach.

Even though they are not technically legally bound by that precedent in that other context, as a matter of good constitutional interpretation, they ought to consider themselves bound by it and ought to change their approach to handling those gag orders. So I think we definitely need a legislative fix.

Unfortunately in this area and a number of areas as you pointed out in your legislation, the administration, any administration saying we are going to look into it or take care of it is not adequate. We need strong rules and clear rules.

Senator FEINGOLD. Ms. Spaulding.

Ms. SPAULDING. I think that's right, Senator. The second circuit was very clear about the constitutional basis for requiring that the government make more than just merely an assertion of the need for secrecy, for example, and I think that is something that carries forward to Section 215 and other contexts in which we have got gag orders in place.

Senator FEINGOLD. I thank you and I thank the Chair.

Senator WHITEHOUSE. Thank you, Senator Feingold. Thank you for your determined and passionate and very thoughtful advocacy in these areas.

Let me start with Ms. Graves' concern that the scope of the 215 authority is very broad in the sense that all the record has to do is pertain to a person and all that person has to have is contact with the target. It could be the butcher at the market, it could be somebody who knows them at work, it could be any sort of thing.

From a point of view of relevance, it would seem logical that the record request in the pertaining to universe would relate in some fashion to the contact. So if we went back to Senator Sessions' example of the U-haul sales person or rental person, if the contact with the target is that they came and rented a U-haul, then it would seem that the logical relevance of records in that U-haul operators universe would be to those dealing with the rental of U-haul to that target.

But there is nothing that I see in the authority that limits it to that. You could go after say school records of the U-haul operator or medical records or phone records or DNA records or any other such thing. I'm wondering given that very broad scope have there been operational guidelines implemented that prevent that sort of thing from happening in the implementation of these statutes and of these requirements to your knowledge, Ms. Spaulding and Mr. Wainstein?

Ms. SPAULDING. I don't know the answer to that, Senator.

Senator WHITEHOUSE. You know, sometimes you've got a very broad legislative authorization but an agency that is implementing it either through administrative rulemaking or through internal procedure narrows it and specifies more precisely in order to keep itself out of trouble, in order to avoid an attack on the statutory authority that they're going to do things in a certain way that is narrower than the full range of their statutory authority.

To your knowledge, has that happened with this particular question pertaining to relevance for somebody who has mere contact with a target?

Mr. WAINSTEIN. Senator Whitehouse, in regards to the 215, the relevance of 215, off the top of my head I can't remember particular internal FBI guidelines that would be a response to your question.

But keep in mind a couple of things. One, the court, we have to make the showing to the court. So built into the statute unlike in the NSL——

Senator WHITEHOUSE. Well, this falls within the presumption that we talked about earlier, doesn't it?

Mr. WAINSTEIN. Yes.

Senator WHITEHOUSE. So once the government has made the showing to the court, the statute says that it is presumptively relevant, the court at that point is faced with an interesting situation because the burden of going forward with showing that it is not relevant has now shifted to a party that is not present in the room, to an imaginary person or a non-existent person.

So where you are the court and you have I think the very awkward situation in front of you unless there is some clarification which is the government is now, or the statute has now moved the burden of going forward and disputing that presumption to a party who does not exist and is not present. So you are kind of stuck with the government's case.

I don't know, the statute would not be any different if you simply said when the government shows you this stuff, you shall issue. I mean, the presumption is a really false linkage. It falsely implies that there is some flexibility there when in fact it is a direct shot because there is nobody to actually claim, to take up the burden of persuasion.

So it is not very reassuring to me to say that well, the judge has a look at it because the judge may very well take the view that hey, I'm stuck with this statutory presumption. If there were somebody here, maybe I could decide between the two parties, particularly if you believe a certain school of judicial activism for the judge to take that step would be, you know, activist because it is not something that is being argued by a party.

The judge is now really hamstrung. So that is not a very reassuring fall back for you, Mr. Wainstein.

Mr. WAINSTEIN. Well, if I may at the risk of sort of wading into the semantic discussion that you had with Mr. Kris. I do understand your concern.

Senator WHITEHOUSE. I thought semantics were important.

Mr. WAINSTEIN. They are important. I understand your concern about the word presumption and how it doesn't really fit in the ex parte context.

It is usually used in the context of two people who are adversarial and they are arguing one way or the other and—the bailout. There is a presumption that someone is a risk of flight or a danger to the community if they are charged with a certain type of violent crime.

That is a presumption that sort of moved the needle over toward the government in the argument as to whether a defendant should be held prior to trial.

Senator WHITEHOUSE. Correct.

Mr. WAINSTEIN. You are very familiar with that. I believe though that it is not inconsistent to apply that same logic to the ex parte context because judges make ex parte decisions all the time.

Let's say in the context of a regular search warrant in a drug case, a judge looks at a search warrant and says OK, I have to look for probable cause. Well, you know, on the meter of burden of proof, probable cause is right here somewhere. So the judge applies that.

Now, there is something to say, there is a presumption on that that moves it over this way and presumably the judge moves that internal needle over to the right a little bit.

So I see your concern about the use of the term that it doesn't really fit. I don't think though that it is inconsistent with sort of standard practice to have judges just be told this is the standard you are going to apply and this standard might change, you know, might rise or lower depending on the existence with certain facts.

If I could just very quickly get to the substance here.

Senator WHITEHOUSE. I'm just not sure that a legal presumption is the technical way that you want to be doing that. I will let you continue, but I just want to summarize. In your testimony, it concludes in very, all or nothing fashion that the roving wire tap authority 215 order authority and the Lone Wolf authority should all be continued. They should be reauthorized.

I don't know that there is any doubt anywhere in this committee that that is the case, so I think the question more is in reauthorizing them, are there further refinements and do I take it from your testimony that it is your belief that there are no further refinements that are appropriate or necessary in any of these provisions?

Mr. WAINSTEIN. No. I would not take my testimony to mean that these provisions are perfect and they should not be touched. I think that the core authorities though are necessary, they are proven to be effective and under sort of the current oversight regimes and with the limitations that are currently built into the statutes, they are being implemented in a way that is consistent with civil liberties.

Senator WHITEHOUSE. I took you off the point that you wanted to make.

Mr. WAINSTEIN. That being said, if there are refinements that could be proposed which would improve the safeguards against misuse but not undermine their effectiveness, and I have heard some ideas here about more public reporting, maybe certain audits, this kind of thing which may very well be very salutary improvements, I'm not objecting to that.

I guess the only point I wanted to make is to kind of reiterate something that David Kris had said earlier when talking about the use of NSLs and 215 orders. Keep in mind that as he said, these are used very early on in an investigation and they are often used to weed out the people who are innocent.

But you are talking about the situation where contact is just sort of a glancing contact and suddenly your records because you happen to be the contacter and the known terrorist is the contactee, your records are now in the possession of the FBI.

In reality, we need that. We need to be able to do that because we have a foreign spy and we see that foreign spy just like we see any—novel sitting on a park bench with a fedora on his head and somebody else walks up with a fedora and a trench coat and sits on that bench and they look very suspicious at 2 in the afternoon, there is good reason to think that maybe that is a drop going on. Some kind of espionage taking place right in that park.

We might want to know something about that guy when he goes and gets in the car and drives away. That's the kind of thing that we need to do early on.

Senator WHITEHOUSE. But then when he gets up from that suspicious meeting and goes down the street and stops in and buys a pack of cigarettes and then goes back out and walks down the street, the poor fellow who just sold him the cigarettes is subject to the exact same degree of scrutiny as the person having the suspicious potential drop meeting and not only in the context of the sale of the cigarettes or even more broadly the operation of that store, but conceivably as to their medical records as to their banking records or as to their, any other kind of personal thing.

It just seems that there might even be an internal relevant standard that would make some, you know, once you are in that world, that the government should still have some burden of showing what they want actually had some relevance to an investigative strategy or theory that the government can articulate before they just go wandering through the bus driver's psychological records. I mean, who knows what it could be. It is a big universe when it is any record pertaining to any person who had any contact with the target. That's a huge universe in this modern world.

Mr. WAINSTEIN. True. Keep in mind however that this has to be explained to a FISA court judge and so the FISA court judge reviewing that factual statement as to what that connection was, and if it is quite clear that it was an obviously innocent day to day interaction, I think you're going to have some questions from the FISA court judge.

Ms. SPAULDING. Although the FISA court judge is limited to applying the law as written as opposed to how the judge thinks it should be written.

Senator WHITEHOUSE. But presumptively the thumb is on the scale in that FISA judge's calculation at that point.

Ms. SPAULDING. The other issue that this raises that is very important of course is that it places a very high premium on having minimization procedures that are very rigorous.

Inevitably you are going to collect records that turn out not to be relevant to your investigation and it is why it is of such concern that the Inspector General found that the minimization procedures for Section 215 were deficient, that they still haven't been issued and that we really weren't able to have a public discussion about those procedures today.

Ms. GRAVES. And if I may, Senator.

Senator WHITEHOUSE. Please.

Ms. GRAVES. On that issue, the standard for national security letters, the same rule applies in essence so long as the records pertain to someone who has any contact without any indicia of suspiciousness, always the hypotheticals involve some suspiciousness.

But the statute doesn't require that that contact have any suspicious element to it.

So for the national security letters of which there have been over 200,000 requests, those require no sort of statement of fact that would show suspiciousness. It merely requires that they show that the record pertain to this person who may have had contact.

The national security letters have been issued in one investigation. There were nine national security letters that covered 11,000 people. This isn't just a hypothetical example of what one degree of separation is. One degree of separation might be 100 people. Two degrees of separation might be 10,000 people. It might be 100,000 depending on how far you wanted to take it.

Of course they don't take it that far but the statute isn't limiting in that way. So the question of requiring that there be something that shows that the records are relevant that the person has engaged in some sort of suspicious activity is important.

When Mr. Comey testified before the House Judiciary committee on this provision in 2005, he said even if you are standing in line at the cafeteria downstairs, he wants to be able to know everything about you and this power allows them to do so. That is why this power is so far reaching and that is why it must be contained.

Senator WHITEHOUSE. Just one other technical point, and let me work off, Ken, your example of the suspicious novel meeting on the park bench. Let's say just for purposes of this example that it had happened not just once but let's say twice, and so there was reasonable grounds for some suspicion that the other individual on the bench might be involved.

Would it not be the case that that other individual at that point could not be designated a target and therefore the universe expands suddenly to now anybody who has contact with the second individual?

I mean, at what point, it is not clear to me at what level of evidence or investigative support the initial designation of who the target is to define the contact with university doesn't grow so that a contact with person now is designated by the government as somebody who has enough suspicion that now we think that they are actually a target themselves and whoosh, now all of their contact with universe gets swept into it.

Is it your view that if there were, the suspicion that you indicated, let's just use those two examples. One meeting on a park bench that has no apparent justification and it looks like a John Lacaray drop type thing or even it being repeated a week later at the same time.

At that point would the second person on the park bench now be able to be designated under the 215 procedure as a target such that anybody with contact with them would be subject to the same 215 inquiries? What is that trigger?

Mr. WAINSTEIN. There are rules. You are probably familiar with the national security guidelines which lay out different levels of investigation. There are full investigations and then there are threat increases and the like that are sort of lesser.

My recollection is that 215, in order to go to the court to get a 215 order, it has to be within the range of a full investigation. There has to be a certain predicate for the FBI to open that.

Senator WHITEHOUSE. Within that investigation the question of who is designated a target versus who is a contact with a target is one that is made administratively by the bureau as I understand it. I don't understand the mechanism or the trigger point at which somebody who is a contact with the target becomes a target themselves.

That's a very small barrier, and it probably should be given the complexity of these investigations, that you contact with universe and they expand very rapidly.

Mr. WAINSTEIN. And I think you have probably been briefed over time as to the FBI's practices in terms of how many hops out from particular known terrorists they go in terms of analyzing relationships. I am not sure how much I can get into at this point.

Senator WHITEHOUSE. Probably not much.

Mr. WAINSTEIN. But the bottom line is there is analysis that goes on there. It is done administratively by the bureau, but there is a relevance standard that has to be met when you go to the FISA court or when you issue an NSL, administratively it has to be satisfied. So the connection can only be so attenuated.

I don't want to go beyond that though in terms of the hop analysis. If I could just get one other point in.

Senator WHITEHOUSE. Please.

Mr. WAINSTEIN. Keep in mind one of the purposes of being able to use these tools, in particular the 215, is to run down a threat that might be about to happen. So you have a scenario for instance where we might well get intelligence that a terrorist is going to be boarding a train from DC to Charlotte and blow that train up with a backpack.

The first thing they will want to do is find out who has booked tickets on that train or an airplane, what have you. That means you are going to issue process to the railroad or the airplane, the airline and say I want to know everybody who is in all those seats.

Well, obviously if it just one target that you are looking for, you are going to be getting information about a lot of people who do not fit within the parameters of that presumption. That is not a tool we can deny investigators.

So if you were to make that, the three part presumption a showing, a mandatory showing of relevance, you preclude the Bureau from having the ability to use the 215 order to get records in that situation which really could be debilitating.

Senator WHITEHOUSE. Yeah, I think that would be debilitating. I would think that the, at that point you have a very different investigative nexus between the threat and the evidence that you seek to secure than you do when the evidentiary nexus is mere contact with.

There you actually have an investigative theory. It is a very clear one and it makes perfect sense for the government to pursue that. If when you get into this contact with theory, it begins to seem a little bit unbounded.

But I want to thank all of you for your testimony. This has been very helpful. I think we are in substantial agreement that there are fine tuning refinements and a variety of audit and accountability measures that are probably appropriate to the statute but

that the fundamental authorities are important to keeping our country safe.

I thank you all for your testimony. The record of the hearing will remain open for another 7 days for anybody who wishes to add to it. But other than that, again my thanks to the witnesses. We are adjourned.

[Whereupon, the hearing was adjourned.]

[Submissions for the record follow.]

SUBMISSIONS FOR THE RECORD

American Association of Law Libraries
MAXIMIZING THE POWER OF THE LAW LIBRARY COMMUNITY SINCE 1906

September 25, 2009

The Honorable Patrick J. Leahy
Chairman of the Judiciary Committee
United States Senate
433 Russell Senate Office Building
Washington, D.C. 20510

Dear Chairman Leahy,

On behalf of the American Association of Law Libraries (AALL), I would like to thank you for introducing The USA PATRIOT Act Sunset Extension Act of 2009 this week and express our support for this important legislation to reauthorize expiring provisions of the USA PATRIOT Act. Your legislation is a carefully crafted bill that is necessary to balance the legitimate needs of the government to use surveillance authorities against threats of terrorism with protecting the constitutional rights of our citizens.

The American Association of Law Libraries (AALL) is a nonprofit educational organization with over 5,000 members nationwide who respond to the information needs of legislators, judges, and other public officials, corporations and small businesses, law professors and students, attorneys and members of the general public. AALL's mission is to promote and enhance the value of law libraries to the legal and public communities, to foster the profession of law librarianship, and to provide leadership in the field of legal information and information policy.

Librarians have been outspoken defenders of the civil liberties and privacy rights of library users since the initial debate over the Act in fall 2001. AALL opposed Section 215, the so-called "library provision," which expanded the Federal Bureau of Investigation's power to require the production of any tangible thing (including books, records, papers, and documents) it claims is "relevant" to authorized foreign intelligence and international terrorism investigations. Section 215 orders come with a gag order which prevents the recipients of the court order from disclosing that fact to anyone other than the attorneys involved in the case and to those who need to know in order to comply with the order.

We are very pleased that your legislation raises the standard for Section 215 orders by requiring that the government demonstrate a connection between the tangible records they seek and a suspected terrorist. We are also pleased that the bill addresses the need for more meaningful judicial review of Section 215 orders and the gag orders accompanying them.

www.aallnet.org
312.939.4764 /PHONE
312.431.1097 /FAX
aallhq@aall.org /EMAIL
105 WEST ADAMS STREET, SUITE 3300
CHICAGO, ILLINOIS 60603

We commend as well your longstanding commitment to raising the standard for obtaining a National Security Letter (NSL) beyond the relevancy requirement. By requiring a higher standard, judicial review and audits of the use of NSLs, your legislation will address the serious misuse of NSL orders as documented in the 2008 report issued by Inspector General Glenn Fine. We are also pleased that your legislation provides the recipient of a NSL gag order a more meaningful opportunity to challenge it, and that it also includes a new four year sunset on NSLs which will ensure the opportunity for legitimate congressional review.

AALL is committed to openness and transparency in government as a means of ensuring public accountability. We applaud the new public reporting provisions requiring more specific information on the use of Section 215 orders and National Security Letters.

We thank you, Chairman Leahy, for your longstanding commitment since the 2001 enactment of the USA PATRIOT Act to narrow many of its overbroad surveillance authorities and closely monitor their use to protect the civil liberties of innocent Americans.

We applaud you for introducing The USA PATRIOT Act Sunset Extension Act of 2009 and for holding the important hearing, "Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security," on September 23. We ask that you please include this letter as part of the record of that hearing. The American Association of Law Libraries strongly supports this important legislation and we look forward to working with you and your staff to ensure its enactment.

Sincerely,

Catherine Lemann

Catherine Lemann
President
American Association of Law Libraries

Statement of the American Civil Liberties Union
Submitted to the Senate Committee on the Judiciary
September 23, 2009

Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security

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

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

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.

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).[13] Under the reauthorization these three provisions, **section 206** and **section 215** of the Patriot Act and **section 6001** of the IRTPA, are all set to expire on December 31, 2009. The 111th Congress will revisit these provisions this year, which creates an opportunity for Congress to examine and evaluate the government's use and abuse of all Patriot Act authorities, as well as 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,[14] 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.[15] 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.[16] 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 hypotheticals having no factual precedent. 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.[17] 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.[18] **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).[19]

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.[20] 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.[21]Most troubling, FBI supervisors used hundreds of illegal "exigent letters" to obtain telephone records without NSLs by falsely claiming emergencies.[22]

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.[23] 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).[24]

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.[25] None of these "blanket NSLs" complied with FBI policy and eight imposed unlawful non-disclosure requirements on recipients.[26] Moreover, the "blanket NSLs" were written to "cover information already acquired through exigent letters and other informal responses."[27] 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.[28] 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.[29] 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."[30] 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.[31]

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).[32] 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.

The ACLU fully supports the National Security Letter Reform Act of 2009 (H.R. 1800) sponsored by Representative Jerrold Nadler (D-NY), as well as the JUSTICE Act introduced by Senators Russ Feingold and Richard Durbin last week, both of which would rein in the FBI's improper use of NSLs. They should be acted upon promptly. Further delay will simply mean that thousands more innocent people will have their private records collected by the FBI.

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.[33]

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."[34] 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.[35] 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.[36]

The IG also discovered the FISC was not the first to raise First Amendment concerns over this investigation to FBI officials. Lawyers with the OIPR raised the First Amendment issue when the FBI sent the section 215 application for its review.[37] 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.[38]

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."[39] 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."[40]

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."[41] 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.[42] 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. 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 the Department of Justice Office of Intelligence Policy Review (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.[43] 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.[44] 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.[45] 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.[46] 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.

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 2009, Congress must once again revisit the Patriot Act, as three temporary provisions from the 2006 reauthorization are set to expire by the end of the year. This time, however, Congress is not completely in the dark. The IG audits ordered in the Patriot Act reauthorization proved the government lied when it claimed that no Patriot Act powers had been abused. Critics 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.

The ACLU's full report documenting abuses under the Patriot Act and suggestions for reform can be found at:
http://www.aclu.org/pdfs/safefree/patriot_report_20090310.pdf.

[1] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
[2] Letter from Ronald Weich, Assistant Attorney General, U.S. Department of Justice, to Senator Patrick Leahy, Chairman, Committee on the Judiciary, (Sept. 14, 2009), *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 v. United States*, 116 U.S. 616 (1886).
[6] *Id.* at 625.
[7] *Id.* at 625.
[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]Pub. L. No. 108-458, 118 Stat. 3638 (2004).
[14] 18 U.S.C. §2518(11), (12).
[15] *Oversight of the Federal Bureau of Investigation: Hearing Before the Senate Judiciary Committee,* 111th Cong. (2009) (Testimony of Robert Mueller, Director, Federal Bureau of Investigation).
[16] Electronic surveillance orders in criminal investigations are governed by the Omnibus Crime Control and Safe Streets Act of 1968. *See* 18 U.S.C.A. §§2510-2520 (2006).
[17] PIRA, *supra* note 16, at § 119(a).
[18] 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).
[19] 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.*
[20] 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].
[21] 2007 NSL Report, *supra* note 22, at 84.
[22] 2007 NSL Report, *supra* note 22, at 86-99.
[23] 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].
[24] 2008 NSL Report, *supra* note 25, at 9.
[25] 2008 NSL Report, *supra* note 25, at 127, 129 n.116.
[26] 2008 NSL Report, *supra* note 25, at 127.
[27] 2008 NSL Report, *supra* note 25, at 127.
[28] 2008 NSL Report, *supra* note 25, at 130.
[29] *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.
[30] 2008 NSL Report, *supra* note 25, at 11, 124.
[31] 2008 NSL Report, *supra* note 25, at 127.
[32] 2008 NSL Report, *supra* note 25, at 81, 88.
[33] 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.
[34] 2008 Section 215 Report, *supra* note 25, at 68.
[35] 2008 Section 215 Report, *supra* note 25, at 72.
[36] 2008 Section 215 Report, *supra* note 25, at 73.
[37] 2008 Section 215 Report, *supra* note 25, at 67.
[38] 2008 Section 215 Report, *supra* note 25, at 72.
[39] 2008 Section 215 Report, *supra* note 25, at 72.
[40] 2008 Section 215 Report, *supra* note 25, at 71 n.63.
[41] 2008 Section 215 Report, *supra* note 25, at 73.
[42] 2008 Section 215 Report, *supra* note 25, at 72-73.
[43] 2008 Section 215 Report, *supra* note 25, at 43.
[44] 2008 Section 215 Report, *supra* note 25, at 45-47.
[45] 2008 Section 215 Report, *supra* note 25, at 47.
[46] *See, Foreign Intelligence Surveillance Act: Closed Hearing Before the H. Permanent Select Comm. on Intelligence,* 110th Cong. (Sept. 6, 2007) (Statement of Kenneth Wainstein, Assistant Attorney General, National Security Division, U.S. Dep't of Justice), *available at* http://www.fas.org/irp/congress/2007_hr/090607wainstein.pdf.

The Constitution Project

September 22, 2009

The Hon. Patrick Leahy
Chairman
Senate Judiciary Committee
United States Senate
Washington, D.C. 20510

The Hon. Jeff Sessions
Ranking Member
Senate Judiciary Committee
United States Senate
Washington, D.C. 20510

Dear Senators Leahy and Sessions and Members of the Senate Judiciary Committee:

The Constitution Project urges the Senate to support the USA Patriot Act Sunset Extension Act of 2009. As debate begins over reauthorization of the three provisions of the Patriot Act set to expire on December 31, 2009, Congress should take this opportunity to ensure that we are protecting not only our security but also our constitutional rights and liberties.

The Constitution Project is a bipartisan organization that promotes and defends constitutional safeguards. The Project brings together legal and policy experts from across the political spectrum to promote consensus solutions to pressing constitutional issues. Today, the Project's Liberty and Security Committee released a report entitled *Statement on Reforming the Patriot Act*. The statement is signed by twenty six policy experts, former government officials, and legal scholars of all partisan affiliations. It calls on Congress to incorporate more robust protections for constitutional rights and civil liberties to reform existing Patriot Act authorities. Specifically, the statement urges that Congress should only reauthorize the three sunsetting provisions – covering business record orders, surveillance of a so-called "lone wolf" terrorist, and "roving" wiretaps – if they are amended to include more robust protections for constitutional rights and civil liberties, and that Congress should revisit and reform two additional Patriot Act provisions covering national security letters and ideological exclusion.

Hastily drafted in the wake of the September 11th attacks, the Patriot Act contains several provisions that give the executive branch extraordinarily broad law enforcement powers and which raise serious constitutional concerns. The Constitution Project is pleased to see the introduction of legislation which targets some of the most troubling provisions of the Patriot Act, particularly the national security letter and business records provisions. The USA Patriot Act Sunset Extension Act of 2009 introduced today is consistent with the recommendations in the Constitution Project's Liberty and Security Committee's report, and passage of this legislation would be an important step toward implementing proper safeguards for constitutional rights.

1200 18th Street, NW, Suite 1000, Washington, DC 20036 202-580-6920 www.constitutionproject.org

Although it is not scheduled to sunset this year, the provision of the Patriot Act in greatest need of reform is the section covering national security letters. Thus the USA Patriot Act Sunset Extension Act's provisions amending the national security letter (NSL) authorities are particularly welcome. The bill would tighten the standards for issuing an NSL, would allow NSL recipients to challenge the nondisclosure or "gag orders" that can accompany NSLs, would add a new four-year sunset on this authority, and would require public reporting on the use of such letters. Importantly, the bill would also reform the business records provision of the Patriot Act, most notably by tightening the standards for obtaining an order compelling a business to turn over records. Finally, the bill would increase public reporting and oversight on the use of these authorities.

In short, the Constitution Project supports the USA Patriot Act Sunset Extension Act because it protects civil liberties while also ensuring law enforcement's ability to protect our national security.

Sincerely,

Sharon Bradford Franklin

Sharon Bradford Franklin
Senior Counsel
The Constitution Project

STATEMENT ON REFORMING THE PATRIOT ACT

A REPORT BY THE CONSTITUTION PROJECT'S LIBERTY AND SECURITY COMMITTEE

September 22, 2009

The Constitution Project
1200 18th Street, NW
Suite 1000
Washington, DC 20036
(202) 580-6920 (tel)
(202) 580-6929 (fax)
info@constitutionproject.org

www.constitutionproject.org

STATEMENT ON REFORMING THE PATRIOT ACT

In October 2001, Congress enacted the USA PATRIOT Act to expand the government's authority to conduct surveillance and search and monitor private records and communications. When Congress reauthorized the Patriot Act in 2006, it made most provisions of the Act permanent, but three provisions are scheduled to sunset on December 31, 2009. These expiring provisions cover business record orders, surveillance of a so-called "lone wolf" terrorist, and "roving" wiretaps.

Since the initial passage of the Patriot Act, we have learned how numerous provisions of the Act intrude upon Americans' privacy rights and civil liberties. Although many parts of the Act were designed to remedy gaps in the United States' intelligence gathering powers, the Patriot Act authorizes overly broad executive powers to track, monitor, and search individuals without adequate safeguards to forestall abuse. In too many instances, such surveillance unnecessarily chills First Amendment freedoms and intrudes upon Fourth Amendment rights.

We, the undersigned members of the Constitution Project's Liberty and Security Committee, agree that the Patriot Act is in need of reform. Some of us would go further, and ask Congress to allow all of the sunsetting provisions to expire, and would also seek repeal of additional Patriot Act provisions. But we are united in urging Congress that it should only reauthorize these three sunsetting provisions if they are amended as outlined below to include more robust protections for constitutional rights and civil liberties. Further, Congress should take this opportunity to revisit and reform two additional Patriot Act provisions covering national security letters and ideological exclusion.

A. THE SUNSETTING PROVISIONS

1. Business Records Provision: Section 215 of the Patriot Act

Section 215 of the Patriot Act, also known as the "business records" or "library records" provision, expanded the FBI's power to obtain material from businesses in connection with counter-terrorism or counter-espionage investigations. It eliminated the prior requirement that the information sought must pertain to an agent of a foreign power, and it expanded the kind of material that could be sought and the entities that could be required to provide information. Under Section 215, the government is required to make only a minimal showing to a judge to obtain an order requiring any person or entity to turn over any document or object. The FBI does not even need to show that the items sought relate to a person the FBI is investigating. The government has to prove only that the information or object sought is relevant to an investigation to protect against international terrorism or espionage. Moreover, Section 215 includes a non-disclosure or "gag order" requirement, allowing the government to effectively bar recipients from disclosing that they have received such orders.

While a judicial order is required before the government can seek records under Section 215, the minimal showing that must be made combined with the broad scope of records that can be obtained makes this power ripe for abuse. As discussed below, we are likewise concerned about the National Security Letter Provision of the Patriot Act, which is not scheduled to sunset.

That provision does not even require a court order and creates similar, but even greater, potential for abuse.

RECOMMENDATIONS:

Congress should amend Section 215 to restore safeguards. These should include all of the following:

a) Tightening the standard for issuing an order under Section 215 to require a showing to a judge of specific and articulable facts demonstrating that the material sought pertains to a suspected agent of a foreign power or a person in contact with or otherwise directly linked to such an agent;

b) Limiting to 30 days the period during which the recipient of a Section 215 order can be required not to disclose existence of the order, unless the government can prove to a judge that there is reason to believe that a specified and articulable harm would result unless the "gag order" is extended; and

c) Requiring adoption of minimization procedures, to ensure that the scope of the order is no greater than necessary to accomplish the investigative purpose.

2. "Lone Wolf" Provision: Section 6001 of the Intelligence Reform and Terrorism Prevention Act

The "lone wolf" provision was originally created to permit surveillance of a hypothetical "lone wolf" terrorist – one who operates without ties to any international terrorist organization. The provision defines "agent of a foreign power" as "any person other than a United States person who engages in international terrorism or activities in preparation therefore . . . ." This provision eliminated the prior requirement in the Foreign Intelligence Surveillance Act (FISA) that surveillance be carried out only against persons suspected of being agents of foreign powers or terrorist organizations. It allows the government to use FISA for surveillance of a non-US person who has no known ties to a group or entity. This authority was further expanded by the amendments enacted last summer which broadened the definition of an "agent of a foreign power" to include individuals "engaged in the proliferation of weapons of mass destruction" even if they are acting alone and are unaware that their actions may be contributing to a WMD effort.

Under FISA, the government can obtain a warrant without a showing of probable cause that a crime is being committed or is about to be committed. FISA's authorization of secret wiretaps and secret home searches in the United States is an exception to traditional Fourth Amendment standards, which has been justified on the basis that these extraordinary surveillance powers are limited to investigations of foreign powers and their agents. By eliminating the requirement to show a connection to any foreign group, the "lone wolf" provision undermines this justification for the lower FISA standards and raises serious constitutional concerns under the Fourth Amendment.

RECOMMENDATION:

Congress should let the "lone wolf" provision sunset due to the serious constitutional issues it raises. Individuals suspected of engaging in terrorism or activities in preparation therefore would still be subject to surveillance and search under traditional and established criminal law standards.

If Congress reauthorizes the "lone wolf" provision it should include a new sunset period together with a rigorous public reporting requirement that would help Members of Congress and the public to assess whether there is any justification for this provision. The new reporting provision should include requirements that the executive branch report on the number of "lone wolf" surveillances authorized and on how many of these targets were charged and prosecuted. This would enable Congress to assess whether surveillance under Title III which is already available for traditional criminal prosecutions is sufficient. Currently, the Attorney General is required to report to Congress semiannually on the use of the "lone wolf" provision; however such reports are not made public.

3. "Roving" Wiretap Provision: Section 206 of the Patriot Act

Section 206 of the Patriot Act allows the government to obtain "roving wiretap" orders that cover multiple phones or email addresses, without citing the particular location of the target. These wiretaps are conducted under FISA and based on orders received from the FISA Court.

This provision was designed to allow surveillance of a target who continually eludes government agents by constantly changing phones and email addresses. However, under Section 206, unlike in traditional criminal investigations, the government is not required to identify *either* the particular communications device to be monitored or the individual who is the subject of the surveillance. The provision does require that the target be described "with particularity," but not that the target be named. Because there is no particularity of location requirement, as traditionally required by the Fourth Amendment, innocent civilians may become inadvertent targets of surveillance.

RECOMMENDATION:

Congress should require that if the wiretap order does not specify the location of the surveillance, then it must identify the target. Conversely, if the order does not specify the target, then it should identify the location with particularity.

B. Additional Problematic Patriot Act Provisions

1. National Security Letter Provision: Section 505 of the Patriot Act

National Security Letters (NSLs) are demand letters signed by officials of the FBI and other agencies, which require disclosure of sensitive information held by banks, credit companies, telephone carriers and Internet Service Providers, among others. No prior judicial approval is required to issue an NSL, and recipients of NSLs are usually prohibited from disclosing the fact or nature of a request.

Section 505 of the Patriot Act eliminated the requirement that the information being sought "pertain to" a foreign power or the agent of a foreign power. This requirement protected information about Americans because few are agents of a foreign government, a foreign terrorist organization, or another foreign power. Instead, today it is sufficient for the FBI merely to assert that the records are "relevant to" an investigation to protect against international terrorism or foreign espionage. Section 505 also eliminated the statutory requirement that agents have any factual basis for seeking records. In addition, Congress has dramatically expanded the types of "financial institutions" on which an NSL can be served to include travel agencies, real estate agents, jewelers, the Postal Service, insurance companies, casinos, car dealers, and other businesses not normally considered "financial institutions."

Audits by the Justice Department Inspector General (IG) released in 2007 and 2008 have revealed numerous abuses in the issuance of NSLs. The IG audits demonstrated that FBI agents had used NSLs in many cases where they were not authorized, including using them against individuals insufficiently related to any FBI investigation and issuing inappropriate "blanket NSLs" in violation of FBI policy. The audits also revealed that the FBI had used "exigent letters" not authorized by law to quickly obtain information without ever issuing the NSL that it promised to issue to cover the request.

Recommendations:

Congress should enact reforms to limit the scope of NSLs and the potential for abuse. These should include all of the following:

a) Requiring that NSLs be used only to obtain records that pertain to suspected terrorists or spies, by re-establishing the prior requirement that there be specific and articulable facts giving reason to believe that the records sought pertain to an agent of a foreign power;

b) Establishing reasonable limits on the "gag" that attaches to an NSL, requiring it to be narrowly tailored and limiting it to 30-days, extendable only by a court and based upon a showing of necessity;

c) Establishing recipients' rights to seek judicial review of NSLs; and

d) Requiring adoption of minimization procedures for information obtained with an NSL to ensure that the scope of the order is no greater than necessary to accomplish the investigative purpose.

2. Ideological Exclusion Provision: Section 411 of the Patriot Act

Section 411 of the Patriot Act expanded the grounds for excluding and deporting foreign nationals based upon speech, raising serious First Amendment concerns. This provision permits the United States to deport foreign nationals for wholly innocent support of a "terrorist organization," even where there is no connection between the foreign national's support and any act of violence, much less terrorism, by the recipient group. It also bars admission to the United States of foreign nationals who "endorse or espouse terrorist activity" or who "persuade others to support terrorist activity or a terrorist organization" in ways determined by the Secretary of State to undermine U.S. efforts to combat terrorism. It also excludes representatives of groups that "endorse acts of terrorist activity" in ways that undermine U.S. efforts to combat terrorism.

These provisions make individuals excludable and removable for speech and association that is constitutionally protected by the First Amendment, and are subject to the same sorts of ideologically biased application that the 1952 McCarran-Walter Act permitted before it was repealed over thirty years later. These provisions were initially cited by the State Department in denying admission to Tariq Ramadan, a Swiss scholar of Islam who had been hired to fill an endowed chair at Notre Dame University.

RECOMMENDATION:

Congress should amend Section 411 to eliminate deportation and exclusion based on speech and association that would be protected by the Constitution if engaged by a United States citizen. When it comes to core First Amendment freedoms, we should not tolerate a double standard.

Members of the Constitution Project's Liberty and Security Committee*

Endorsing the Statement on Reforming the Patriot Act

CO-CHAIRS:

David Cole, Professor, Georgetown University Law Center

David Keene, Chairman, American Conservative Union

MEMBERS:

Stephen E. Abraham, Partner, Fink & Abraham LLP; Lieutenant Colonel, Military Intelligence, United States Army Reserve (Ret)

Azizah al-Hibri, Professor, The T.C. Williams School of Law, University of Richmond; President, Karamah: Muslim Women Lawyers for Human Rights

Bob Barr, Former Member of Congress (R-GA); CEO, Liberty Strategies, LLC; the 21st Century Liberties Chair for Freedom and Privacy, American Conservative Union; Chairman, Patriots to Restore Checks and Balances; Practicing attorney; United States Attorney for the Northern District of Georgia, 1986-1990

Christopher Bryant, Professor of Law, University of Cincinnati; Assistant to the Senate Legal Counsel, 1997-99

Phillip J. Cooper, Professor, Mark O. Hatfield School of Government, Portland State University

John W. Dean, White House Counsel, Nixon Administration

Mickey Edwards, Lecturer, Woodrow Wilson School of Public and International Affairs, Princeton University; former Member of Congress (R-OK) and Chairman of the House Republican Policy Committee

Thomas B. Evans, Jr., Former Member of Congress (R-DE) and Co-Chairman of the Republican National Committee; Founder, Florida Coalition for Preservation

Eugene R. Fidell, Florence Rogatz Visiting Lecturer in Law, Yale Law School

Louis Fisher, Specialist in Constitutional Law, Law Library, Library of Congress

Michael German, Policy Counsel, American Civil Liberties Union; Adjunct Professor, National Defense University School for National Security Executive Education; Special Agent, Federal Bureau of Investigation, 1988-2004

Melvin A. Goodman, Senior Fellow, National Security Project, Center for International Policy

Morton H. Halperin, Senior Advisor, Open Society Policy Center

David Lawrence, Jr., President, Early Childhood Initiative Foundation; former Publisher, *Miami Herald* and *Detroit Free Press*

Thomas R. Pickering, Undersecretary of State for Political Affairs, 1997-2000; United States Ambassador and Representative to the United Nations, 1989-1992

L. Michael Seidman, Professor, Georgetown University Law Center

Earl Silbert, Partner, DLA Piper; United States Attorney, District of Columbia, 1974-1979; Former Watergate Prosecutor

Neal Sonnett, Chair, American Bar Association Task Force on Treatment of Enemy Combatants and Task Force on Domestic Surveillance in the Fight Against Terrorism; former President, National Association of Criminal Defense Lawyers; former Assistant United States Attorney for the Southern District of Florida

Geoffrey Stone, Harry Kalven, Jr. Distinguished Service Professor of Law, the University of Chicago Law School

James A. Thurber, Director and Distinguished Professor, Center for Congressional and Presidential Studies, American University

Charles Tiefer, General Counsel (Acting), 1993-94, Solicitor and Deputy General Counsel, 1984-95, U.S. House of Representatives

Don Wallace, Jr., Professor, Georgetown University Law Center; Chairman, International Law Institute, Washington, DC

John W. Whitehead, President, the Rutherford Institute

Roger Wilkins, Clarence J. Robinson Professor Emeritus, George Mason University; Director of U. S. Community Relations Service, Johnson Administration

---

CONSTITUTION PROJECT STAFF:

Sharon Bradford Franklin, Senior Counsel

---

[*] *Affiliations listed for identification purposes only*

Statement of the Constitution Project Submitted to the Senate Judiciary Committee in Connection with the September 23, 2009 Hearing on Reauthorizing the USA Patriot Act: Ensuring Liberty and Security

September 29, 2009

The Constitution Project submits this statement to urge Congress to enact critical reforms to the USA Patriot Act, to ensure that we protect both national security and Americans' privacy rights and civil liberties. As Congress considers the three provisions of the Patriot Act set to expire on December 31st – those covering business record orders, surveillance of a so-called "lone wolf" terrorist, and "roving" wiretaps – it should take the opportunity to revisit and reform these provisions and others that fail to include proper safeguards to protect individual rights. In particular, the provision governing national security letters (NSLs) should be reformed. Passage of the USA Patriot Act Sunset Extension Act of 2009 would be an important step toward serving these goals.

The Constitution Project is a bipartisan organization that promotes and defends constitutional safeguards. The Project brings together legal and policy experts from across the political spectrum to promote consensus solutions to pressing constitutional issues. In advance of this year's reauthorization of the Patriot Act, the Constitution Project's Liberty and Security Committee released a report entitled *Statement on Reforming the Patriot Act*. The statement is signed by twenty six policy experts, former government officials, and legal scholars of all partisan affiliations. It calls on Congress to amend the Patriot Act to include more robust protections for constitutional rights and civil liberties and provides specific policy recommendations. The USA Patriot Act Sunset Extension Act, introduced last week, is consistent with these recommendations, and we fully support his proposals for reform.

The History of the Patriot Act and the Need for Reform

The Patriot Act was hastily drafted in the wake of the September 11th terrorist attacks and contained many provisions which granted new, extraordinarily broad law-enforcement powers to the executive branch. The Patriot Act contains provisions that allow the government to conduct surveillance and gather documents from third parties, in some instances without being required to first seek judicial approval. Some of these provisions contain "gag" orders, preventing third parties who receive orders to turn over documents from disclosing that they have received such an order.

Granting the executive branch such unfettered law enforcement authority raises serious constitutional concerns, and in fact we have seen abuses of this authority in the eight years since the Patriot Act was passed. For example, audits by the Justice Department Inspector General (IG) released in 2007 and 2008 have revealed numerous abuses in the issuance of national security letters (NSLs). The IG audits demonstrated that FBI agents had used NSLs in many cases where they were not authorized, including using them against individuals insufficiently related to any FBI investigation and issuing

inappropriate "blanket NSLs" in violation of FBI policy. The audits also revealed that the FBI had used "exigent letters" not authorized by law to quickly obtain information without ever issuing the NSL that it promised to issue to cover the request. Such abuses will be perpetuated unless Congress acts to reform the Patriot Act to bring it in line with tradition constitutional norms.

Key Reforms in the USA Patriot Act Sunset Extension Act of 2009

National Security Letters

- **Standard for Obtaining an NSL:** Under current law, a national security letter can be obtained by simply having an official certify that the information sought is relevant to an authorized investigation. Section 6 of the USA Patriot Act Extension Act of 2009 would require the official to also provide a statement of facts showing that there is reason to believe the information sought is relevant to an authorized investigation. This is a critical reform, although the Constitution Project recommends that Congress go even further, and require that the government provide specific and articulable facts showing that there is reason to believe the records sought *pertain to an agent of a foreign power.*

- **Limitations on the Duration of "Gag" Orders**: Section 4 of the USA Patriot Act Extension Act of 2009 would strip the government of the power to issue "gag" orders of indefinite duration in connection with an NSL. The bill would allow the government to issue a nondisclosure order lasting no longer than one year, with the order being renewable for one-year intervals thereafter if the government is able to demonstrate the continued need for nondisclosure. While the Constitution Project's report goes even further and recommends limiting the duration of nondisclosure orders to 30 days, extendable only by a court based upon a showing of necessity, this provision of the USA Patriot Act Sunset Extension Act would be an important step forward in ending indefinite gag orders.

- **Judicial Review of "Gag" Orders:** Currently, the Patriot Act does not provide for judicial review of nondisclosure orders attached to NSLs. Section 5 of the bill would establish a procedure by which the recipient of an NSL can challenge the validity of the nondisclosure order. The Constitution Project supports this effort to provide meaningful judicial review of nondisclosure orders.

- **Sunset Provisions**: Section 2 of the USA Patriot Act Extension Act of 2009 establishes a sunset date for the NSLs provision. The NSL provision is not presently scheduled to sunset, and adding a new sunset date would help promote a vigorous system of checks and balances. The establishment of a sunset provision would allow Congress to revisit the NSL provision in 2013 to further assess the need for reform.

Business Records Provision

- **Standards for Accessing Business Records:** Section 215 of the Patriot Act allows the government access to "certain business records" held by third parties if those records are relevant to a foreign intelligence or international terrorism investigation. Before the Foreign Intelligence Surveillance Act (FISA) court will grant an agent the authority to issue such an order, the government must demonstrate that the records it seeks are in fact relevant to an authorized investigation. However, under current law, records are presumptively relevant. Section 3 of the USA Patriot Act Sunset Extension Act would eliminate this presumption, and would require the government to make a factual showing to support the issuance of a Section 215 order, including facts showing that the records sought pertain to an agent of a foreign power or a person in contact with such an agent. This reform is consistent with the Constitution Project's recommendations for tightening the standard for issuing Section 215 orders and would provide meaningful judicial review of this broad law enforcement power.

- **Judicial Review of Nondisclosure Orders:** Under current law, the recipient of an order under Section 215 must wait a year to challenge the validity of a nondisclosure order. Section 5 of the bill would allow the recipient of an order issued under Section 215 the right to challenge a nondisclosure order as soon as it is received.

- **Minimization:** Section 5 of the USA Patriot Act Sunset Extension Act would require that a FISA court approve minimization procedures in any instance where the collection of business records under section 215 involves the gathering of information concerning a U.S. person. This would further the Constitution Project's recommendation for the adoption of robust minimization procedures to ensure that the scope of orders issued under Section 215 is no greater than necessary to accomplish the investigative purpose.

Lone Wolf and Roving Wiretap Provisions

- **Sunset Provisions:** Section 2 of the USA Patriot Act Extension Act of 2009 would set a new sunset period for the "lone wolf" and roving wiretap provisions. These new sunsets would ensure further close oversight by Congress, and are therefore welcome reforms. In its report, *Statement on Reforming the Patriot Act,* the Constitution Project recommends further reforms to these provisions, such as requiring detailed and public reporting on the use, if any, of the lone wolf provision. This is especially important now in light of the Department of Justice's recent admission that it has never found it necessary to use this provision.

Requirements for Public Reporting and Audits

- **Public Reporting:** The bill would require annual public reporting on the use of NSLs as well as public reports on the aggregate numbers of requests for surveillance under FISA that includes breakdowns by category of surveillance. These provisions would help promote effective oversight and accountability.

- **Audits:** Section 9 of the USA Patriot Act Extension Act would require additional audits of the use of NSLs, and audits on the use of Section 215 orders, by the Justice Department's Inspector General. The 2007 and 2008 audits were extremely helpful in revealing abuses of the NSL authority. This provision would provide a critical tool to promote accountability and avoid future abuses.

In short, the USA Patriot Act Sunset Extension Act of 2009 would provide key reforms to safeguard constitutional values and civil liberties, while still giving law enforcement the tools to effectively investigate terrorists. The Constitution Project looks forward to seeing Congress enact these important reforms.

Sharon Bradford Franklin
Senior Counsel
Constitution Project
1200 18th Street, NW
Suite 1000
Washington, DC 20036
202-580-6920

Senate Judiciary Committee
Hearing on
"Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security"
Wednesday, September 23, 2009

Statement of U.S. Senator Russell D. Feingold

At the end of this year, three provisions of the USA PATRIOT Act will sunset unless Congress acts to reauthorize them. In my view, Congress should take this opportunity to revisit not just those three provisions, but rather a broad range of surveillance laws enacted in recent years to assess what additional safeguards are needed.

That is why I have introduced the JUSTICE Act, S. 1686, along with Senator Durbin and eight other Senators. It takes a comprehensive approach to fixing the USA PATRIOT Act and the FISA Amendments Act, once and for all. It permits the government to conduct necessary surveillance, but within a framework of accountability and oversight. It ensures both that our government has the tools to keep us safe, and that the privacy and civil liberties of innocent Americans will be protected. Because as the title of this hearing suggests, we can and must do both. These are not mutually exclusive goals.

Indeed, the Department of Justice just last week acknowledged as much in a letter setting forth its views on Patriot Act reauthorization. The Department said: "We also are aware that Members of Congress may propose modifications to provide additional protection for the privacy of law abiding Americans. As President Obama said in his speech at the National Archives on May 21, 2009, 'We are indeed at war with al Qaeda and its affiliates. We do need to update our institutions to deal with this threat. But we must do so with an abiding confidence in the rule of law and due process; in checks and balances and accountability.' Therefore, the Administration is willing to consider such ideas, provided that they do not undermine the effectiveness of these important authorities."

I welcome the administration's openness to potential reforms of the Patriot Act and look forward to working together as the reauthorization process moves forward this fall.

But I remain concerned that critical information about the implementation of the Patriot Act has not been made public – information that I believe would have a significant impact on the debate. During the debate on the Protect America Act and the FISA Amendments Acts in 2007 and 2008, critical legal and factual information remained unknown to the public and to most members of Congress – information that was certainly relevant to the debate and might even have made a difference in votes. And during the last Patriot Act reauthorization debate in 2005, a great deal of implementation

information remained classified. This time around, we must find a way to have an open and honest debate about the nature of these government powers, while protecting national security secrets.

As a first step, the Justice Department's letter made public for the first time that the so-called "lone wolf" authority – one of the three expiring provisions – has never been used. That was a good start, since this is a key fact as we consider whether to extend that power. But there also is information about the use of Section 215 orders that I believe Congress and the American people deserve to know. I do not underestimate the importance of protecting our national security secrets. But before we decide whether and in what form to extend these authorities, Congress and the American people deserve to know at least basic information about how they have been used. So I hope that the administration will consider seriously making public some additional basic information, particularly with respect to the use of Section 215 orders.

Mr. Chairman, there can be no question that statutory changes to our surveillance laws are necessary. Since the Patriot Act was first passed in 2001, we have learned important lessons, and perhaps the most important of all is that Congress cannot grant the government overly broad authorities and just keep its fingers crossed that they won't be misused, or interpreted by aggressive executive branch lawyers in as broad a way as possible. Congress has the responsibility to put appropriate limits on government authorities – limits that allow agents to actively pursue criminals, terrorists and spies, but that also protect the privacy of innocent Americans.

This lesson was most clear in the context of National Security Letters. In reports issued in 2007 and 2008, the Department of Justice Inspector General carefully documented rampant misuse and abuse of the National Security Letter (NSL) authority by the FBI. The Inspector General found – as he put it – "widespread and serious misuse of the FBI's national security letter authorities. In many instances, the FBI's misuse of national security letters violated NSL statutes, Attorney General Guidelines, or the FBI's own internal policies." After those Inspector General reports, there can no longer be any doubt that granting overbroad authority leads to abuses. The FBI's apparently lax attitude and in some cases grave misuse of these potentially very intrusive authorities is attributable in no small part to the USA PATRIOT Act. That flawed legislation greatly expanded the NSL authorities, essentially granting the FBI a blank check to obtain some very sensitive records about Americans, including people not under any suspicion of wrong-doing, without judicial approval. Congress gave the FBI very few rules to follow, and should not be all that surprised at the result.

This time around, we have the opportunity to get this right. That is why we should look at a range of issues and not just the three provisions that expire. I look forward to working with every member of this committee to that end.

Statement of

Glenn A. Fine
Inspector General, U.S. Department of Justice

before the
Senate Committee on the Judiciary

concerning

Reauthorizing the USA Patriot Act
September 23, 2009

Mr. Chairman, Ranking Member Sessions, and Members of the Judiciary Committee:

Thank you for inviting me to testify about the Office of the Inspector General's (OIG) oversight work related to reauthorization of the USA Patriot Act. Our most significant oversight work regarding the Patriot Act has focused on the Federal Bureau of Investigation's (FBI) use of national security letters (NSL) and Section 215 orders to obtain business records, and I will focus primarily on those issues in my testimony today.

In 2005, the Patriot Reauthorization Act directed the OIG to review the FBI's use of NSLs and Section 215 orders. In March 2007, the OIG issued reports examining the FBI's use of Section 215 orders and NSLs, which found serious misuse of NSL authorities. By contrast, we found that Section 215 orders generally were not subject to misuse, although they were used much less frequently than NSLs. A second set of reports, issued in March 2008, again examined the use of Section 215 orders and NLS, including the measures taken or proposed by the FBI and the Department of Justice (Department) to address the OIG's recommendations regarding the misuse of NSLs.

In this written statement, I first summarize the findings of our NSL and Section 215 reports. I also provide an update on the status of the OIG's ongoing review of the FBI's previous use of so-called "exigent letters" rather than NSLs to obtain telephone records. I then discuss the actions the FBI and the Department have taken in response to our recommendations, including the FBI's creation of an Office of Integrity and Compliance and oversight of the FBI's use of NSLs by the Department's National Security Division.

Finally, I briefly discuss other OIG work related to the Patriot Act, including the OIG's responsibilities under Section 1001 of the Patriot Act to examine allegations of civil rights and civil liberties complaints against Department employees. I also note several ongoing and recently completed

OIG reviews that, while not directly related to the Patriot Act, affect the FBI's ability to perform its important mission.

I. SUMMARY OF FINDINGS OF OIG REPORTS ON THE FBI'S USE OF NATIONAL SECURITY LETTERS FROM 2003 – 2006

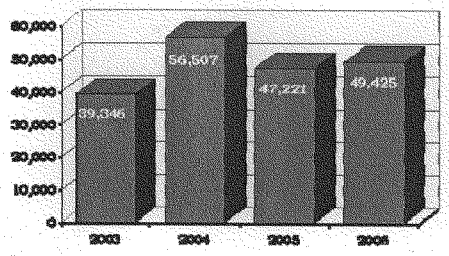
As required by the Patriot Reauthorization Act, the OIG examined the FBI's use of NSLs from 2003 to 2006. As discussed in our two reports, the FBI is authorized under five statutory provisions to use NSLs to obtain records such as telephone toll billing records and subscriber information from communication service providers, transactional records from Internet service providers, bank records from financial institutions, and consumer credit information from credit reporting agencies.

The original Patriot Act in 2001 significantly broadened the FBI's authority to use NSLs by both lowering the threshold standard for issuing them and by expanding the number of FBI officials who could sign the letters. First, the Patriot Act eliminated the requirement that the information sought must pertain to a foreign power or an agent of a foreign power. Instead, it substituted the lower threshold standard that the information requested must be relevant to or sought for an investigation to protect against international terrorism or espionage. In addition, the Patriot Act permitted Special Agents in Charge (SAC) of the FBI's 56 field offices to sign national security letters, which significantly expanded approval authority beyond the previously limited number of FBI Headquarters officials. The Patriot Act also added a new authority allowing NSLs to be used to obtain consumer full credit reports in international terrorism investigations.

Our NSL reports examined the effectiveness of NSLs, which are used by the FBI for various purposes, including developing evidence to support applications for orders issued under the *Foreign Intelligence Surveillance Act* (FISA), developing links between subjects of FBI investigations and other individuals, providing leads and evidence to allow FBI agents to initiate or close investigations, and corroborating information obtained by other investigative techniques. During both of our NSL reviews, FBI personnel told us that they believe NSLs are indispensable investigative tools in many counterterrorism and counterintelligence investigations.

Our review of the FBI's use of NSLs from 2003 – 2006 identified a general upward trend in their use, with the FBI issuing more than 192,000 NSL requests during this 4-year period.

National Security Letter Requests (2003 through 2006)



However, the OIG found that these statistics, which were based on information from the FBI's database, significantly understated the total number of NSL requests issued by the FBI because the FBI's tracking database was inaccurate and did not include all NSL requests. For example, our examination of case files at four FBI field offices found approximately 22 percent more NSL requests in the case files that we examined than were recorded in the database for those same files.

Our reports recognized the significant challenges the FBI faced and the major organizational changes it was undergoing during our review period. Nevertheless, we concluded that the FBI engaged in serious misuse of NSL authorities. For example, from 2003 to 2005 the FBI identified 26 possible intelligence violations involving its use of NSLs. The possible violations included issuing NSLs without proper authorization and making improper requests under the statutes cited in the NSLs.

However, in addition to the possible violations reported by the FBI, we conducted an independent review of FBI case files in four field offices to determine if there were unreported violations of NSL authorities, Attorney General Guidelines, or internal FBI policies governing the approval and use of NSLs. Our review of 293 national security letters in 77 files found 22 possible violations that had not been identified or reported by the FBI. The violations we found fell into three categories: improper authorization for the NSL, improper requests under the pertinent national security letter statutes, and unauthorized collections.

Examples of the violations we identified included issuing NSLs for consumer full credit reports in a counterintelligence case, which is not statutorily permitted; issuing an NSL for a consumer full credit report when the FBI Special Agent in Charge had approved an NSL for more limited credit information under a different NSL authority; issuing an NSL when the investigation had lapsed; and obtaining telephone toll billing records for

periods in excess of the time period requested in the NSL due to third-party errors.

Thus, it is significant that in the limited file review we conducted of 77 investigative files in 4 FBI field offices, we identified nearly as many NSL-related violations (22) as the total number of possible violations that the FBI had identified (26) in reports from all FBI Headquarters and field divisions over the 3-year period. Moreover, 17 of the 77 files we reviewed (22 percent) had 1 or more violations.

Most troubling, the OIG's March 2007 review also identified more than 700 instances in which the FBI improperly obtained telephone toll billing records and subscriber information from communication service providers by issuing so-called "exigent letters" signed by personnel in the FBI's Counterterrorism Division rather than by issuing proper NSLs. These exigent letters stated they were being issued due to exigent circumstances and the FBI was in the process of obtaining subpoenas for the requested information. However, the OIG found that in some instances there was no pending investigation associated with the request at the time the exigent letters were sent; many were not issued in exigent circumstances; the FBI was unable to determine which letters were sent in exigent circumstances due to inadequate recordkeeping; and subpoenas in many instances had not, in fact, been submitted to the U.S. Attorneys Offices as represented in the exigent letters. As a result of our review, the FBI ended its practice of using exigent letters. As I discuss in more detail later in this statement, the OIG is in the final stages of our review that assesses who was responsible for the misuse of exigent letters and other improper requests for telephone records.

The OIG's March 2007 report on NSLs made 10 recommendations to the FBI, including improving its database to ensure that it captures timely, complete, and accurate data on NSLs; issuing additional guidance to field offices to assist in identifying possible intelligence violations arising from the use of NSLs; and taking steps to ensure that it employs NSLs in accordance with the requirements of NSL authorities, Department guidelines, and internal policy. The FBI concurred with all of our recommendations and agreed to implement corrective actions.

One year later, in March 2008, the OIG issued a follow-up review on the FBI's use of NSLs in which we determined that the FBI and the Department had made significant progress implementing recommendations from our first report and adopting corrective actions to address the serious problems we identified. The measures implemented by the FBI included developing a new NSL data system designed to facilitate the issuance and tracking of NSLs and ensure accurate reports to Congress and the public on NSL usage; issuing NSL guidance memoranda and conducting training of field and headquarters

personnel; and creating a new FBI Office of Integrity and Compliance, an internal oversight office modeled after private sector compliance programs.

We also found that the FBI had devoted substantial time and resources to ensure that its field managers and agents understood the seriousness of the FBI's shortcomings in its use of NSLs and their responsibility for correcting these deficiencies. In addition, in response to our March 2007 findings the Department's National Security Division instituted periodic national security reviews of FBI field and Headquarters divisions to assess whether the FBI was using various intelligence techniques, including NSLs, in accordance with applicable laws, guidelines, and policies.

Our March 2008 report also examined whether NSLs issued after the effective date of the Patriot Reauthorization Act contained the required certifications to impose non-disclosure and confidentially requirements on NSL recipients. In the random sample of NSLs we reviewed, we found that 97percent of the NSLs imposed non-disclosure and confidentiality requirements and almost all contained the required certifications. We found that some of the justifications for imposing this requirement were perfunctory and conclusory, and that a small number of the NSL approval memoranda failed to comply with internal FBI policy.

Our March 2008 report made 17 additional recommendations to improve the FBI's use and oversight of NSLs, such as providing additional guidance and training for FBI agents on the proper use of NSLs and on the reviewing, filing, and retention of NSL-derived information; reinforcing the need for FBI agents and supervisors to determine whether there is adequate justification for imposing non-disclosure and confidentiality requirements on NSL recipients; regularly monitoring the preparation and handling of NSLs; and providing timely reports of possible intelligence violations to FBI Headquarters. The FBI agreed with the recommendations and said it would implement additional actions to address our findings.

II. SUMMARY OF FINDINGS OF OIG REPORTS ON THE FBI'S USE OF SECTION 215 REQUESTS FOR BUSINESS RECORDS FROM 2002 – 2006

As also directed by the 2005 Patriot Reauthorization Act, the OIG issued two reports on the FBI's use of Section 215 orders to obtain business records. Section 215 of the Patriot Act allows the FBI to seek an order from the Foreign Intelligence Surveillance Court to obtain "any tangible thing," including books, records, and other items from any business, organization, or entity if the item is for an authorized investigation to protect against international terrorism or clandestine intelligence activity. This is one of the three provisions that "sunsets" in December 2009 and is a focus of this hearing.

Our first report on the use of Section 215 orders, issued in March 2007, examined the FBI's use of Section 215 authority from 2002 through 2005. We found that the Department's Office of Intelligence Policy and Review, on behalf of the FBI, submitted requests for two different types of Section 215 applications to the FISA Court: "pure" Section 215 applications and "combination" Section 215 applications. A "pure" Section 215 application referred to a Section 215 application for any tangible item that was not associated with any other FISA authority. A "combination" Section 215 application referred to a Section 215 request that was added to a FISA application for pen register/trap and trace orders, which identify incoming and outgoing telephone numbers called on a particular line.

We found that from 2002 through 2005 the Department, on behalf of the FBI, submitted to the FISA Court a total of 21 pure Section 215 applications and 141 combination Section 215 applications. We found only two instances involving improper use of these Section 215 orders, which involved overcollections in response to Section 215 combination pen/register trap and trace orders. In both instances, the FBI identified the overcollections and reported the matter to the FISA Court and the Intelligence Oversight Board (IOB).

Our report also found that the FBI has not used Section 215 orders as effectively as it could have because of legal, bureaucratic, or other impediments to obtaining these orders. For example, we found significant delays within the FBI and the Department in processing requests for Section 215 orders. We also determined through our interviews that FBI field offices did not fully understand Section 215 orders or the process for obtaining them.

Our follow-up report issued in March 2008 examined the FBI's use of Section 215 orders in 2006. We found that in 2006 the FBI and the Department processed 15 "pure" Section 215 applications and 32 "combination" Section 215 applications that were formally submitted to and approved by the FISA Court. Six additional 215 applications were withdrawn by the FBI before they were formally submitted to the FISA Court.

In both of our reports, we found no instance in which the information obtained from a Section 215 order resulted in a major case development. However, FBI personnel said that the importance of information from Section 215 orders is sometimes not known until much later in an investigation – for example, when the information was linked to some other piece of intelligence. We also found that little of the information obtained through Section 215 orders had been disseminated to intelligence agencies outside the Department. Nevertheless, FBI personnel told us that Section 215 authority was essential to national security investigations because it was the only compulsory process for certain kinds of records that could not be obtained through alternative means, such as NSLs or grand jury subpoenas.

Our March 2008 review did not identify any illegal use of Section 215 orders in 2006. However, we found two instances when the FBI received more information than it requested in the Section 215 orders. In one case, approximately 2 months passed before the FBI recognized it was receiving additional information that was beyond the scope of the FISA Court order. The FBI reported this incident to the IOB, and the additional information was sequestered with the FISA Court. In the other case, the FBI quickly determined that it inadvertently received information not authorized by the Section 215 order and isolated the records. However, the FBI concluded that the matter was not reportable to the IOB and that it should be able to use the material as if it were "voluntarily produced" because the information was not statutorily protected. We disagreed with this conclusion, and our report recommended that the FBI develop procedures for identifying and handling information that is produced in response to, but outside the scope of, Section 215 orders.

In addition, our report discussed another case in which the FISA Court twice refused to authorize a Section 215 order based on concerns that the investigation was premised on protected First Amendment activity. However, the FBI subsequently issued NSLs to obtain information about the subject based on the same factual predicate and without a review to ensure the investigation did not violate the subject's First Amendment rights. We questioned the appropriateness of the FBI's actions because the NSL statute contains the same First Amendment caveat as the Section 215 statute.

Of the three recommendations we made in our 215 reports, the FBI has addressed one recommendation, partially addressed a second recommendation, and has yet to address the third.

First, we recommended that the FBI develop procedures for reviewing materials received from Section 215 orders to ensure that it has not received information not authorized by the FISA Court orders. In response, the FBI developed a policy that requires the case agent to review material produced pursuant to a Section 215 order to determine whether the materials produced were responsive to the 215 order prior to uploading the material into FBI databases.

Second, we recommended that the FBI develop procedures for handling material that is produced in response to, but outside the scope of, a Section 215 order. The FBI responded by stating that it would sequester overproduced material that is "statutorily protected." However, the FBI's policy allows agents to treat non-statutorily protected material as "voluntarily produced" without any inquiry whether the overproduced material was inadvertently or voluntarily produced.

We disagree with the FBI's position on this matter for several reasons. The collections under a Section 215 order can involve non-public information about U.S. persons who are not the subject of national security investigations, and the FBI often uploads such information into FBI databases. The FBI's comparison of a Section 215 order to a grand jury subpoena or civil discovery request is misplaced because, unlike a grand jury subpoena or civil discovery request, a Section 215 order is issued by the FISA Court. Moreover, unlike in the civil or grand jury context, it is unlikely that the persons or entities whose interests are affected by the overproduced records in response to a Section 215 order will learn that information about them has been uploaded into the FBI's databases. We also believe that the distinction that the FBI makes – between statutorily protected records and non-statutorily protected records – when a provider produces records beyond that which is called for by the Section 215 order should not be dispositive as to whether the records are uploaded into the FBI's databases. Finally, we do not believe that it is so difficult or burdensome for the FBI to inquire with the provider whether the records were produced inadvertently (which will likely be the cases in many instances) or, in the alternative, to obtain a Section 215 order for the overproduced material.

Our third recommendation related to the minimization procedures that the Patriot Reauthorization Act required the Department to implement for records obtained pursuant to Section 215 orders. The Reauthorization Act required specific procedures designed for Section 215 material that would minimize the retention and prohibit the dissemination of non-publicly available information concerning United States persons consistent with national security interests. The Reauthorization Act required that these procedures be adopted by September 5, 2006.

However, there was disagreement between the Department and the FBI regarding the definitions and scope of minimization procedures in general, including the time period for retention of Section 215 records, and whether to include procedures for addressing information received in response to but beyond the scope of the Section 215 order. To meet the statutory deadline, the Department adopted sections of the Attorney General Guidelines for FBI National Security Investigations and Foreign Intelligence Collections of October 31, 2003 (Guidelines) as "interim" minimization procedures for business records.

In our March 2008 Report, we concluded that these interim minimization procedures were deficient. The interim procedures were not specific to Section 215 records -- in fact, compliance with the Guidelines was already a prerequisite to obtaining a Section 215 order. In our report, we again recommended that the Department continue to work to develop appropriate standard minimization procedures for Section 215 records.

According to the FBI, the Department has drafted new minimization procedures for business records. However these procedures have not been issued.

III. OIG's EXIGENT LETTER INVESTIGATION

As noted above, perhaps the most troubling finding in our review of the FBI's use of NSLs involved the use of exigent letters. In our 2007 NSL report, we found that from March 2003 to November 2006 personnel in the FBI's Communications Analysis Unit (CAU) issued at least 722 exigent letters to three communication service providers seeking telephone records. Most of the letters stated that the records were requested "due to exigent circumstances" and that grand jury subpoenas for the records had been "submitted to the U.S. Attorney's Office who will process and serve them formally. . . as expeditiously as possible."

Yet, contrary to the assertions in the exigent letters, subpoenas requesting the telephone records in many instances had not been provided to the U.S. Attorney's Office before the letters were issued. We also interviewed witnesses who told us that the FBI sometimes used exigent letters in non-emergency circumstances.

The Electronic Communications Privacy Act (ECPA) prohibits communication service providers from disclosing telephone records to the government unless compelled to do so by legal process such as an NSL, or pursuant to the voluntary emergency disclosure provision of ECPA, 18 U.S.C. Section 2702(c)(4). We concluded that the exigent letters did not constitute valid legal process under ECPA. We also were not persuaded by the FBI's justification of the letters under the emergency voluntary disclosure provision for several reasons, including that the letters were sometimes used in non-emergency circumstances and that senior FBI attorneys told us they did not rely on the emergency voluntary disclosure provision to authorize the letters at the time. We concluded that the FBI's use of exigent letters to obtain telephone records was an improper circumvention of ECPA.

After issuance of our NSL report, we conducted a separate review to examine in detail the FBI's use of exigent letters and other informal requests for telephone records, and also to determine who in the FBI was accountable for these improper uses. The OIG has completed a draft report regarding the misuse of exigent letters, as well as other informal requests such as oral and e-mail requests to the service providers for telephone records. In addition, we reviewed the FBI's issuance of after-the-fact NSLs to "cover" or validate records the FBI had received pursuant to exigent letters and other informal requests. Our report examines the accountability of FBI agents, supervisors, lawyers, and managers who used or condoned the use of these exigent letters and other informal requests for records.

In April 2009, pursuant to the OIG's normal process, we provided the FBI and the Department our draft report and asked for comments on its factual accuracy and whether any information in the report was classified or too sensitive for public release. The FBI's response was delayed, and subsequently the Office of the Director of National Intelligence (ODNI) became involved and consulted with other intelligence agencies in conducting a classification and sensitivity review. We recently received these comments from the FBI and ODNI, and we have made available an unclassified version of the report to subjects of the review for their comments. We will provide our report to the Committee and issue it publicly as soon as it is completed.

IV. ASSESSMENT OF THE FBI'S AND DEPARTMENT'S RESPONSES TO THE OIG REPORTS

In this section, I discuss the FBI's and the Department's responses to our NSL reports. Although we have not yet conducted another follow-up review of the FBI's response to our reports, we have been monitoring the FBI's implementation of our recommendations. For example, the OIG has met with officials from the FBI's National Security Law Branch and others staff within the FBI's Office of General Counsel and with officials in the FBI's Office of Integrity and Compliance to discuss their actions to institute corrective actions. We also have been briefed on the new NSL data management subsystem that the FBI deployed last year to address some of the problems we identified in our NSL reports. In addition, we have reviewed internal audits conducted by the FBI Inspection Division, which concluded that there has been a decrease in several types of administrative errors in the use of NSLs that we described in our reports.

We also met with officials in the Department's National Security Division who are regularly examining the FBI's performance regarding the use of NSLs in its counterterrorism and counterintelligence investigations.

In the following sections, I offer the OIG's thoughts on the FBI's and the Department's responses to the findings in our reports. In general, our sense is that the FBI is taking seriously its need to implement corrective action and to ensure that controls are implemented to prevent the serious violations our reports disclosed.

A. FBI Corrective Actions

The FBI has taken a series of actions in an effort to address our recommendations regarding NSLs. For example, in January 2008 the FBI deployed a new NSL computer subsystem built on the same computer application used to manage its Foreign Intelligence Surveillance Act (FISA) data. The NSL subsystem is now in use in all FBI field offices and at FBI

Headquarters. This new system standardizes and automatically tracks NSL requests by creating mandatory fields for NSLs that must be completed by the requesting FBI case agent or official before a request to issue an NSL can be routed for review and approval by FBI supervisors, Chief Division Counsel, and Special Agents in Charge. This new process should eliminate discrepancies between NSL requests and approval documents and, among other information, also maintain a record of the U.S. person status of each target of an NSL request. While this subsystem will not eliminate all instances of non-compliance with NSL requirements, it has reduced common errors in NSLs that were identified in our reports, and it also has enhanced the FBI's ability to accurately track NSLs and compile reports to Congress and other oversight entities.

In response to our recommendations that the FBI improve guidance and training with respect to the NSL process, in December 2008 the FBI issued a comprehensive Domestic Investigations and Operations Guide. According to the FBI, this Guide is being used to provide intensive training throughout the FBI on the proper use of investigative authority in general and supplements and reinforces the more focused training on the use of NSLs already being provided.

In response to our concern that the FBI was issuing NSLs contrary to statutory limitations, AG Guidelines, or internal FBI guidance, the FBI reported that its Inspection Division will periodically review a sample of NSLs to examine whether the necessary showing of relevance is made in each cover document accompanying an NSL and whether other actions are taken in compliance with NSL authorities and FBI policies. We have been told that the Inspection Division intends to conduct such audits on a quarterly basis, although it has not yet begun to conduct these quarterly reviews.

In addition, in response to the serious violations we found in our two NSL reports the FBI created an Office of Integrity and Compliance (OIC) in 2007 which is modeled after private sector compliance programs. According to the FBI, the OIC's purpose is "to develop, implement, and oversee a program that ensures there are processes and procedures in place that promote FBI compliance with both the letter and spirit of all applicable laws, regulations, and policies." The FBI reported that the OIC will establish policies on compliance standards, guide assessments of FBI programs to determine areas at risk of non-compliance, and develop training for FBI employees that will mitigate those risks. The OIC will also work with the FBI Inspections Division to identify high-risk areas and ensure that compliance monitoring is carefully planned and executed. At present, the OIC is staffed by 15 personnel, and includes 9 attorneys, 3 program analysts, 1 administrative assistant, 1 special agent/attorney (on an 18-month detail), and 1 Assistant Director.

We believe this office can perform a valuable function by providing a process for identifying problem areas throughout the FBI, assessing existing FBI control mechanisms, and developing and implementing better internal controls on FBI procedures, including its use of NSLs. However, the OIC's responsibilities cover all operational and program areas in the FBI, and we do not believe this office should be looked to as the primary oversight mechanism to ensure proper use of NSLs and Section 215 orders.

In addition, in our March 2008 report we recommended that the FBI consider providing the OIC with a larger permanent staff. The small size of the OIC remains a concern to us because at its present strength it cannot independently conduct risk assessments of FBI's operations. Instead, the OIC relies on staff from the responsible program offices – the "risk owners" – to self-identify those areas of their operations most at risk of non-compliance with laws or regulations. We are concerned that relying on self-identification rather than aggressive independent review can result in assessments that focus on already known problems and miss unknown or emerging risks. Further, relying on program personnel to identify risks and conduct the compliance reviews puts the program personnel in the potentially difficult position of criticizing their FBI colleagues and supervisors.

Because of the importance of the OIC and the emphasis the FBI has placed on this office in addressing the problems we found in our NSL reports, the OIG intends to initiate a separate review to assess in detail the work of this office.

We also believe that additional work is needed to address other concerns we raised in our reports. For example, in our NSL reviews we recommended that the FBI consider changing the reporting structure for Chief Division Counsel (CDCs), the chief lawyers in each FBI field office. FBI Division Counsel play a critical role in reviewing and approving NSLs. Chief Division Counsel are responsible for identifying and correcting erroneous information in NSLs and NSL approval memoranda, resolving questions about the scope of the NSL statutes, ensuring adequate predication for NSL requests, and providing advice on issues concerning the collection of any unauthorized information through any national security letters.

Chief Division Counsel report to the Special Agents in Charge of the field offices in which they work, not to the Office of General Counsel (OGC) at FBI Headquarters. As a result, personnel decisions such as performance reviews, compensation, and promotion determinations concerning Chief Division Counsel are made by the Special Agents in Charge. We also found in our review that because Division Counsel report primarily to SACs rather than to FBI OGC, some Chief Division Counsel are reluctant to question NSL requests or to challenge requests generated in the course of field office investigations.

We understand that the FBI recently has taken steps to open Chief Division positions to non-agent attorneys and that other chain-of-command changes are under consideration, but at present the FBI has not modified the reporting structure for Chief Division Counsel. We believe this is a significant issue that should be addressed, and we remain concerned that Chief Division Counsel still report to and are supervised by their Special Agents in Charge, and therefore the Chief Division Counsel may not always provide the independent and rigorous review needed of the decision to approve NSLs.

B. National Security Division Corrective Actions

Our March 2008 report noted that the Department's National Security Division (NSD) has implemented additional measures to seek to ensure better compliance with NSL authorities. For example, in 2007 the NSD began reviews, modeled in part on the file reviews conducted by the OIG in our first NSL report, to examine whether the FBI is using various intelligence techniques including NSLs in accordance with applicable laws, guidelines, and policies. In conjunction with the FBI's Office of General Counsel, NSD attorneys review national security investigation files at the FBI. Among other things, the reviews examine FBI compliance with Attorney General national security investigation guidelines, use of NSLs, predication for national security investigations, and referrals to the Intelligence Oversight Board.

To date the NSD has conducted approximately 43 reviews, including 38 reviews of FBI field offices, 3 follow-up reviews of previously visited field offices, and 2 reviews of FBI Headquarters components. By the close of 2010, the NSD plans to complete reviews at all 56 FBI field offices and at FBI Headquarters.

NSD officials told us that they have observed during these reviews a significant decline in compliance issues with regard to NSLs, particularly since the FBI implemented its NSL data subsystem. However, the NSD reviews have identified areas of continuing concern, including FBI personnel not consistently following FBI guidance that material collected as a result of third party overproductions should not be uploaded into FBI databases or used to further the investigation pending review by Chief Division Counsel, and failures to specify in NSL approval documents the relevance of records sought to authorized national security investigations.

C. Department NSL Working Group

In response to the 2005 Patriot Reauthorization Act and the recommendations in our first NSL report, the Attorney General formed a Working Group (NSL Working Group) to examine how NSL-derived information is used and retained by the FBI. The Working Group was also charged with proposing minimization procedures that would ensure the FBI's collection of

information through NSLs and its retention of NSL-derived information was limited to the minimum necessary to carry out its counterterrorism mission.

In August 2007, the NSL Working Group sent the Attorney General its report and proposed minimization procedures. However, we had several concerns with the findings and recommendations of the Working Group's report, which we discussed in our March 2008 NSL report. In particular, we disagreed with the Working Group about the sufficiency of existing privacy safeguards and measures for minimizing the retention of NSL-derived information. We disagreed because the controls the Working Group cited as providing safeguards predated our NSL reviews, yet we found serious abuses of the NSL authorities.

As a result, the Acting Privacy Officer decided to reconsider the recommendations and withdrew them. The Working Group has subsequently developed new recommendations for NSL minimization procedures, which are still being considered within the Department and have not yet been issued. We believe that the Department should promptly consider the Working Group's proposal and issue final minimization procedures for NSLs that address the collection of information through NSLs, how the FBI can upload NSL information in FBI databases, the dissemination of NSL information, the appropriate tagging and tracking of NSL derived information in FBI databases and files, and the time period for retention of NSL obtained information. At this point, more than 2 years have elapsed since after our first report was issued, and final guidance is needed and overdue.

V. OTHER OIG REPORTS

I also want to briefly highlight several OIG reviews that may be of interest to the Committee. In addition to requiring OIG reviews of the FBI's use of NSLs and Section 215 orders, Section 1001 of the Patriot Act directed the OIG to undertake a series of actions related to claims of civil rights or civil liberties violations allegedly committed by DOJ employees. Specifically, Section 1001 required the OIG to "review information and receive complaints alleging abuses of civil rights and civil liberties by employees and officials of the Department of Justice." It also required the OIG to provide semiannual reports to Congress on the implementation of the OIG's responsibilities under Section 1001. The OIG has issued 15 Section 1001 reports since enactment of the legislation in October 2001. These OIG reports describe the allegations of civil rights and civil liberties abuses we received during each 6-month period and how we handled them.

The OIG has also conducted numerous other reviews of the FBI that, while not directly involving Patriot Act authorities, relate to FBI programs and functions that can impact its ability to perform its vital missions. For example, the OIG is continuing a series of ongoing reviews examining the FBI's

development of its Sentinel case management project. The Sentinel program is intended to upgrade the FBI's electronic case management system to improve the FBI's ability to use and share case information. Since March 2006, we have issued four audits reports that focus on the planning and development of Sentinel, the FBI's processes and controls for managing Sentinel, and the contract with Lockheed Martin to develop Sentinel. We are nearing completion of our fifth audit on these issues.

In addition, the OIG has conducted reviews of the accuracy of the FBI's terrorist watchlist and the FBI's role in connection with the President's Surveillance Program.

The OIG also is conducting a follow-up review of where the FBI has allocated its investigative resources. In the aftermath of the September 11, 2001, terrorist attacks, the FBI underwent a broad transformation aimed at focusing the agency on terrorism and intelligence-related matters. The OIG issued three previous audit reports examining how the FBI has managed this reprioritization and the impact it has had on the FBI's more traditional criminal investigations. Our current audit is examining whether the FBI has improved its process for allocating resources among its various operations and is also examining the changes in the FBI's allocation of resources during the past 3 years.

In addition, we are nearing completion of a follow-up audit of the FBI's foreign language translation program. This review is assessing the FBI's ability to translate foreign language information it receives and whether the FBI ensures the appropriate prioritization of translation work, accurate and timely translations of pertinent information, and adequate pre- and post-hire security screening of linguists. This review is also examining the FBI's success in meeting linguist hiring goals and the extent of any translation backlogs and the efforts taken by the FBI to address these backlogs.

VI. CONCLUSION

In sum, the Patriot Act gave the FBI significant new powers to perform its vital counterterrorism and counterintelligence missions. Our reviews found that, with regard to the use of national security letters, the FBI did not initially take seriously enough its responsibility to ensure that these letters were used in accord with the law, Attorney General Guidelines, or FBI policies. Since our disclosure of the abuses of NSLs, we believe that the FBI has devoted significant time, energy, and resources to correcting its errors, and has also attempted to ensure that its employees understand the seriousness of the FBI's shortcomings with respect to its use of national security letters and the FBI's responsibility for correcting these deficiencies.

However, this is an ongoing process and it is too early to definitively state whether the FBI's efforts have eliminated the problems we found with its use of these authorities. We also believe that as Congress considers reauthorizing provisions of the Patriot Act, it must ensure through continual and aggressive oversight that the FBI uses these important and intrusive investigative authorities appropriately. We believe this oversight should come from several different levels and from different entities – not only congressional oversight hearings, but also rigorous oversight by FBI Headquarters managers and by FBI field supervisors, and regular oversight by the Department's National Security Division. The OIG also has an important role to play in this oversight process, and we intend to continue our reviews of the FBI's use of Patriot Act authorities, including NSLs and Section 215 orders.

That concludes my prepared statement. I would be pleased to answer any questions.

Statement of Lisa Graves[1]
Executive Director
Center for Media and Democracy[2]
Before the
United States Senate Judiciary Committee
September 23, 2009

Reforming the USA PATRIOT Act and Expanded Surveillance of Americans

Chairman Leahy, Ranking Member Sessions, and Members of the Senate Judiciary Committee, thank you for the opportunity to testify today.

I am pleased to endorse the improvements in the Patriot Act Sunset Extension Act that was introduced this week by Senator Leahy, a staunch defender of liberty and security. He was right to vote against the deeply flawed Patriot Act expansion in 2006, and his determination to begin this reform of these powers is worthy of support. These reforms are an important down-payment toward restoring liberties that have been lost. I hope these and additional reforms of federal surveillance powers that have been excessively expanded will be adopted by Congress and signed into law by President Obama.

I. These Powers Are About Us, About Who We Are as Americans

Let me begin with someone far braver and more eloquent than me, Captain Ian Fishback, a U.S. soldier in Iraq who challenged the abuse of prisoners and wrote about "the larger question that this generation will answer":

> Do we sacrifice our ideals in order to preserve security? Terrorism inspires fear and suppresses ideas like freedom and individual rights. Overcoming the fear posed by terrorist threats is a tremendous test of our courage. Will we confront danger and adversity in order to preserve our ideals, or will our courage and commitment to individual rights wither at the prospect of sacrifice? My response is simple. If we abandon our ideals in the face of adversity and aggression, then those ideals were never really in our possession. I would rather die fighting than give up even the smallest part of the idea that is "America."[3]

I agree that we must transcend the fear others want to trigger in our hearts, and we need to summon tremendous courage to help preserve and restore ideals that truly make America the land of the free.

---

[1] I previously served as Deputy Director of the Center for National Security Studies (CNSS), the Senior Legislative Strategist for the American Civil Liberties Union (ACLU), the Chief Nominations Counsel for Senator Leahy, the Deputy Chief of the Article III Judges Division of the U.S. Courts, and Deputy Assistant Attorney General in the Office of Legal Policy/Office of Policy Development at the U.S. Department of Justice. I am indebted to the work of my former colleagues with the ACLU—Michelle Richardson, Mike German, and Jeani Murray of the legislative office and Ann Beeson, Jameel Jaffer, Melissa Goodman who were litigating these issues during my tenure there, among other devoted civil libertarians—my former partner, Kate Martin, of CNSS who has been challenging these issues since before 2001, intelligence expert Suzanne Spaulding whom I am testifying alongside today, and other great civil liberties advocates in the national security surveillance coalition I have helped lead since the 2005 debate over Patriot Act reauthorization and in the ongoing challenges to warrantless wiretapping. I would also like to thank Kate Rhudy for her assistance with this testimony and all her help over the past two years as my law clerk and now as a lawyer. My testimony reflects my own views, of course, and any mistakes are my own.

[2] The Center for Media and Democracy, which was founded by John Stauber in 1993, is an independent, non-profit, non-partisan public interest organization dedicated to promoting transparency and informed debate by exposing government propaganda and corporate spin. Among our priorities is countering misinformation by investigating public relations campaigns by the government and informing grassroots citizen activism that promotes human rights as well as other policies to make the world a better place. CMD's investigations have been praised by leading journalists, such as Amy Goodman of Democracy Now! who observed that "The Center's work in exposing government and corporate propaganda is absolutely essential to our democracy."

[3] Quoted by Andrew Sullivan in THE ATLANTIC, "Dear President Bush" (October 2009).

One of the challenges in this area is whether we have the will to see beyond a particular investigation or crisis, press for the truth, insist on answers, and demand the strong checks and balances that are essential to the idea of America. One of the most important reasons our system of government is so successful, why our democracy has endured, is that we set limits on government power. Elected leaders and government bureaucrats are bounded by the Constitution, laws passed by Congress, and the availability of review of actions taken by independent courts staffed with impartial judges. Checks on power help guarantee that we stay a free country, but these important checks have been greatly eroded.

That is why Americans from all walks of life have stood up against actions by a handful of leaders and operatives who acted in secret and in violation of our laws—with practices like monitoring Americans without court warrants or any proof of wrongdoing, detaining people in secret prisons without redress by the courts, and torture. The Chairman was right to call for a truth commission to ensure that there is accountability to our system of government. Unfortunately, that common sense call has been rebuffed, and the vacuum left by the lack of accounting has been filled with self-serving claims that these policies "work." And, there has been precious little space to have a real conversation about better alternatives that would be both more effective and more consistent with needed checks and balances.

While some of the powers at issue allow people to be monitored without any proof of wrongdoing, the government always concedes that conducting surveillance of everyone is not possible or efficient. But that concession masks the true extent and the true costs of the massive web of secret surveillance of Americans that has been erected over the past several years. Due to the cloak of secrecy that envelopes these powers, it is difficult to picture what is really happening behind closed doors. And, we want to believe that government agents are focused only on the bad guys, but the record tells a different story. Not only does evidence show that many innocent Americans are being secretly swept in, but also the record shows this is happening *because* of recent changes to how the law is written or interpreted, not in spite of the law. Meanwhile, key facts have been kept hidden or been disclosed quite selectively, while other "facts" have turned out to be deliberately misleading, if not outright lies or propaganda. That is one of the reasons that while this debate is often cast in terms of the other, the enemy, it is more properly focused on what we stand *for* as a free people, what our rules should be for surveillance in *this* country, and whether we will call out misinformation and demand the truth as sovereign citizens.

II. The Current Patriot Act Debate and What Should Be on the Table

Today's hearing is focused on the three provisions designated by the Patriot Act reauthorization bill to be up for renewal this year: Section 215, secret orders for records or information about you held by third parties; Section 206, secret roving wiretaps; and the so-called "lone wolf" provision. Rather than adopt this format, I am going to focus on how some of the powers set to expire relate to broader issues at stake and other provisions that should be on the table. I simply do not think this White House and this Congress should accede to the agenda for this debate dictated by the Republican-controlled Congress and White House in 2006. Other secret surveillance powers that undermine Americans' privacy can and should be on the table, and so I would urge this Committee, this Congress, and the new Administration not to feel bound by the narrow topics teed up back in 2006 for debate today.

That is one of the reasons I am very appreciative of the Chairman's decision to include changes to the National Security Letter (NSL) provisions expanded by Section 505 of the Patriot Act and by the 2006 reauthorization, among others. I hope a majority of this Committee will support Senator Feingold's amendments to sensibly update the standards for issuing NSLs and revise other powers that are dangerously overbroad or unjustified, as detailed in his JUSTICE Act. (I am especially proud to be here as a new constituent of Senator Feingold, who bravely stood alone against Patriot in 2001.)

A. Domestic Surveillance that Undermines the Privacy of Americans' Personal Records

1. § 215 Orders Cover Any Tangible Thing and Require No Wrongdoing by You

One way to think of the scope of the power covered by Section 215 of the Patriot Act is to think of a giant file into which literally "any tangible thing" held by a third party about you can be put, that is, can be secretly obtained by government agents. Any tangible thing. It could be your DNA, your genetic code, from tests taken by your doctor for your health. It could be records about the books you buy or read. It could be information about websites you have visited. To search your home for these types of personal records, the government would have to have a warrant based on probable cause of wrongdoing, but to obtain them from your doctor or others you do business with, such as your internet service provider or your employer, no such probable cause is required under the statute since 2001.

In fact, any tangible thing about you can be secretly obtained without any evidence that you are a suspected terrorist. Virtually everything about you can be seized through secret 215 orders if you have any contact with a suspect. On the surface that might sound reasonable, but when you think it through you can see that every day through work or business you come into contact with dozens of people, at work, at schools, at conferences, in the cafeteria, at sporting events, at the mall, and if any one of them is the subject of an investigation your sensitive, personal private information might get swept up and kept in government files for decades. That amounts to hundreds of people a year and mere contact, however brief, can trigger this law, which requires the secret Foreign Intelligence Surveillance Court to presume your sensitive personal records are relevant to an investigation and grant a secret access.

And, under the law as amended in 2006, your employer, doctor, or librarian, for example, who may have known you since childhood, cannot ever tell you your privacy has been breached without going to court, even if you are never charged with any wrongdoing. And, it bars them from even challenging such orders for your personal, private information for a year. And, even then, the law as amended in 2006 makes it almost impossible for that person or business to prevail, by creating a conclusive presumption against disclosure if a government official certifies the request should be kept secret for various reasons, without providing the court with any facts to test such assertions.

It is no wonder that librarians and booksellers and other groups devoted to protecting freedom of conscience strongly oppose these far-reaching and excessive secret powers. At every juncture, the prior administration eliminated checks and balances that would help protect the innocent and ensure these powers were properly focused. Senator Leahy's bill would require that the government provide facts showing why they think the records they are seeking are actually relevant rather than just show any contact with a subject of an investigation, and it would allow recipients to challenge orders for the disclosure of any tangible thing sought. These changes would untie the court's hands in assessing the original request and any challenge to it or to the related gag order. Senator Feingold's bill would make similar changes and also require that any restriction on freedom of speech related to receiving such an order be narrowly tailored, in accordance with First Amendment law, and it would allow the use of these tangible things to be challenged in court just like any other evidence. Both bills would also require more court oversight of how the things obtained with these orders are used or disseminated.

These are important steps toward containing and refocusing this far-reaching power. In my view, to better protect innocent Americans, this power should be predicated on more than mere contact—it should require some reason to believe the subject is knowingly aiding a suspect rather than merely in the wrong place at the wrong time while engaged the innocent business of daily life. Congress should also probe the findings of the Inspector General that, after a rare denial of a requested Section 215 order, the FBI circumvented the court by using an NSL and should prevent this from happening again.

2. Extreme Secrecy Was Used to Obscure the Truth and Distort the Debate

The Section 215 power was subjected to a sunset, or time limit, back in 2001 because it was a newly created, far-reaching power. In the debate over the Patriot Act in 2005, the Bush Administration made a deliberate decision to voluntarily de-classify statistics about how infrequently this power was used. The power had been used only a few dozen times, and this fact was used to attack opponents as over-reacting to the potential danger of this power. Since then, the government has used this power much more regularly, resulting in a ten-fold increase in Section 215 orders in just two years.

At the same time, the administration adamantly refused to disclose the number of demands for third party records being issued under the changes made by Section 505 of the Patriot Act, which is known as the National Security Letter (NSL) power. NSLs were not made subject to the sunset in 2005 because they were a power that pre-dated the Patriot Act, even though those powers were greatly expanded in 2001. One way to think about the relationship between Section 215 orders for any tangible thing and Section 505 demands for information about financial transactions, phone records, internet transactions (who you e-mail and who e-mails you), and credit reporting information is to think of a circle within a circle. Everything covered by a Section 505 demand also counts as a tangible thing under Section 215, but not every tangible thing is a financial, internet, phone, or credit record.

However, notwithstanding the dangers of permissive access to any tangible thing about you without any showing of probable cause, Section 505 NSLs are even more dangerous to individual liberty. This is because NSLs are issued by the FBI without any court approval whatsoever. These are unilateral, coercive, and secret demands by FBI agents to businesses for personal, private information about you, without even having to show the secret FISA court in Washington any evidence supporting the request. So, of course, we in the civil liberties community believed these powers were being widely used. And, even though this controversial power became a major part of the reauthorization debate in 2005, the administration refused to make public even the number of requests made, while touting the assertion that it had used the related Section 215 powers sparingly, only a handful of times. The ACLU filed a FOIA request for the numbers and ended up with six-page document in which nearly every entry related to the number of NSLs was redacted except for the words "Grand Total." It literally took an act of Congress to dislodge the information about how often NSLs had been used, through required audits and reporting, which were some of the only real improvements made in the deeply flawed 2006 reauthorization of the Patriot Act.

But, in November 2005 as the Patriot Act was being delayed by a mounting filibuster in the Senate, an investigative piece by the Washington Post's Bart Gellman quoted government sources reporting that the number of NSL requests had exploded to over 30,000 per year.[4] The Justice Department harshly attacked the article in a letter to then-Chairman Specter signed by William Moschella, and calling the 30,000 figure "inaccurate." I myself heard from a number of staff and reporters that the administration had absolutely denied that anywhere near this number of demands had been made, just as the NSL powers were being debated on the Hill and in public. Congress responded to the controversy by requiring an audit of the number of times the power was being used.

That is how in 2007 we learned that the true number of NSL requests issued in 2004, the year before the article was published, was over 56,000.[5] The number reported in the press was not too big; it was

[4] Barton Gellman, "The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans" WASHINGTON POST, A01 (Sunday, November 6, 2005).

[5] For my detailed assessment of the 2007 NSL audit, *see* www.intelligence.house.gov/Media/PDFS/Graves032807.pdf.

too small! The administration attempted to sidestep this dispute by asserting that its statements were based on counting only the number of letters and not the number of requests. Yet, administration officials had to know that individual letters often had multiple requests. To this day, there has been no real accountability for the way the public was misled by DOJ at the crucial moment in this debate. In another instance of deliberately distorting the public debate in 2005, while the prior administration was asserting that the government was not interested in library records it was simultaneously seeking records from the Library Connection in Connecticut and gagging those librarians from telling Congress and rebutting the misleading assertions of the government. Both the Leahy and Feingold bills amend the law to address the constitutional flaws noted by the U.S. Court of Appeals for the Second Circuit in that case regarding the gag order that accompanies an NSL. These improvements are essential.

3. Weakened Standards for NSLs Have Swept in Numerous Innocent People

The Department of Justice's own Annual Performance and Accountability Report in 2006 described in stark terms how the current standards for using NSLs affect ordinary Americans:

> Likewise, investigative and intelligence authorities enacted or expanded in the Patriot Act [and the 2005 reauthorization] invest broad new information-gathering powers in FBI agents and their supervisors . . . on a minimal evidentiary predicate. For example, . . . it authorized the FBI to collect information such as telephone records, Internet usage, and credit and banking information on persons who are not subjects of FBI investigations. This means that the FBI—and other law enforcement or Intelligence Community agencies with access to FBI databases—is able to review and store information about American citizens and others in the United States who are not subjects of FBI foreign counterintelligence investigations and about whom the FBI has no individualized suspicion of illegal activity.

www.usdoj.gov/ag/annualreports/pr2006/2006par.pdf (adding that therefore these powers need "aggressive oversight" internally).

The Feingold bill redresses this problem with an important update to NSLs to require the bare minimum that should be required in a free society: that the FBI have individualized suspicion about the person records it wants pertain to, instead of permitting an internal government assertion or boilerplate certification of relevance to an "authorized investigation." This is critically important because the Executive Branch re-wrote the rules to allow a "preliminary inquiry" to count as an authorized investigation, even though the statute intended that these intrusive powers only be used when a full investigation was underway, which required at least some evidence of a reasonable likelihood of wrongdoing. Even the FBI Director conceded to Senator Wyden in 2005 that these newly renamed "preliminary investigations" had "no particular standard of proof." (And, I would strongly urge the Committee to look more closely at the revised AG Guidelines for investigations, which also need to be changed to protect against increased monitoring of First Amendment activities.)

Under the current weakened "standard," as the Inspector General noted, the FBI has used NSLs to obtain information about people two or three degrees of separation away from the target/subject of an investigation. This is important for ensuring that these powers are sensibly focused. Assuming, conservatively, that an average person is in contact with a hundred people between family, friends, co-workers, and merchants, two degrees of separation is 10,000 people (100 x 100)—and, it is documented that one investigation in 2004 alone used a nine NSLs to obtain information about over 11,000 people. And, three degrees of separation could sweep in 100,000

people (10,000 x 100). It is far too permissive and unreasonable to allow these intrusive powers such a broad, almost arbitrary reach into Americans' lives and communities.

It is also the case that FBI agents told the Inspector General that NSLs were very useful in clearing people and closing files, but the FBI General Counsel has asserted that private records about people who are cleared be kept for perpetually, purportedly to help clear them again. Indeed, in 2007, the Inspector General made clear that nothing in DOJ or FBI policies require "the purging of information derived from NSLs in FBI databases, regardless of the outcome of the investigation. Thus, once information is obtained in response to a national security letter, it is indefinitely retained and retrievable by the many authorized personnel who have access to various FBI databases." How many of the people subject to the over NSL requests are innocent? We do not know for certain, but we do know that the government conducts only a couple dozen international terrorism prosecutions per year, according to the Transactional Records Access Clearinghouse.

4. The Number of NSL Requests Dwarf the Number of 215 Orders

Cumulatively, we know that over 230,000 NSL requests have been issued in the past eight years, but even this number is too low. Despite receiving a personal assurance by the Director of the FBI that some reasonable estimate of the of NSLs issued in 2001 and 2002 would be made public, those numbers remain undisclosed. Plus, the figures reported for 2007 and 2008 exclude the number of NSL requests for internet transaction information. So, the true number could be 300,000, more or less.

Even that number would not include any NSLs that were withdrawn or threatened, as Gellman reported occurred when Las Vegas casinos shared over 1,000,000 hotel records in late 2003/early 2004. (Hotel/casinos were swept into the NSL powers when the law was amended to construe "financial institution" to include casinos, as well as insurance companies, jewelers, boat sellers, and the U.S. Postal Service, among other institutions that are not banks but that have some cash business.) Those figures are not included in the statistics, which demonstrates how even mandatory reporting about the mere numbers of NSLs can be sidestepped through other tools, such as "voluntary" compliance with requests, the use of grand jury subpoenas, and grounded or groundless assertions of emergency or exigency, none of which currently require public reporting and which should be fixed. This also underscores a little-noticed fact that has emerged: NSLs are not the exclusive means for obtaining Americans' financial, credit, internet, or phone records. This creates uncertainty for agents and a real lack of adequate controls to protect the public. Fortunately, the Feingold bill includes a provision to ensure that the FBI's unlawful use of so-called exigent letters is barred and emergencies are bona fide.

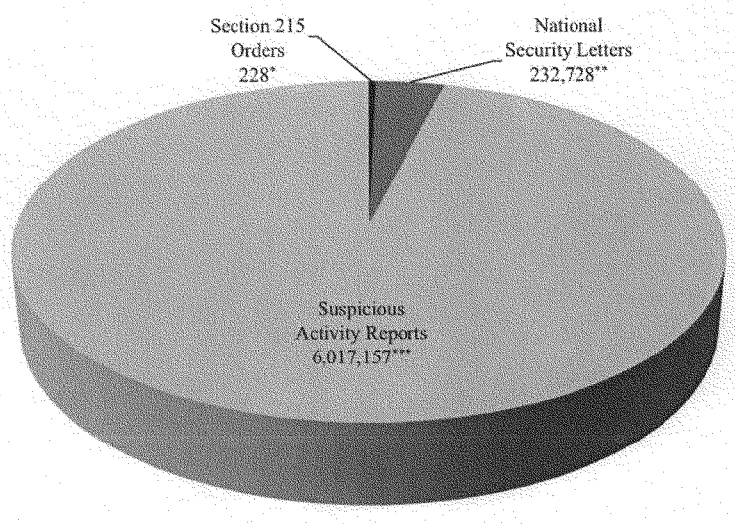
Even assuming the 230,000 figure were not significantly understated, the number of 215 orders is dwarfed by the number of NSL demands. At a minimum, there are almost a thousand NSLs issued for every 215 order issued. NSLs are affecting tens of thousands more people in the U.S. than Section 215 orders, and yet the focus on the expiring powers is effectively distracting from the more widely used NSLs. Additionally, NSLs are being used increasingly against United States citizens who now represent the majority of individuals about whom and NSL has been issued. (In 2006, 60% of NSLs were about U.S. persons, compared with approximately a third in 2003.)

5. And, the Number of NSLs Is Dwarfed by Suspicious Activity Reports

Title III of the Patriot Act expanded immunity and incentives for financial institutions to secretly file Suspicious Activity Reports (SARs) on their customers. SARs are sent from banks, for example, to the U.S. Department of the Treasury, which transmits these reports to the FBI for inclusion in the Investigative Data Warehouse. Even though SARs are not issued by the government, they are part of

the broader issues resulting in the tremendous expansion in FBI files about ordinary Americans. Most of the hearings about this issue have featured government witnesses talking about connecting the dots and stopping the flow of terrorist money. But, little has been done to examine the exponential growth in the number of private financial records being secretly and voluntarily shared with the government. Back in 2000, the number of SARs was about 160,000 per year, and the annual figure has increased ten-fold in less than a decade, with over 1.2 million issued in 2007 alone.

Section 215 Represents a Tiny Slice of the Data FBI Is Now Collecting



Sources for chart data (with thanks to the ACLU's recent report on the Patriot Act):
* U.S. 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 77 (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703a/final.pdf (number of Section 215 orders in 2001 through 2005); U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006, 84 (Mar. 2008), *available at* http://www.usdoj.gov/ oig/special/s0803a/final.pdf (number of Section 215 orders in 2006); Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney General, U.S. Department of Justice, to Nancy Pelosi, Speaker, U.S. House of Representatives (Apr. 30, 2008), *available at* http://www.fas.org/irp/ agency/doj/fisa/2007rept.pdf (number of Section 215 orders in 2007); Letter from Ronald Weich, Assistant Attorney General, U.S. Department of Justice, to Harry Reid, Majority Leader, U.S. Senate (May 14, 2009), *available at* http://www.fas.org/irp/ agency/doj/fisa/2008rept.pdf (number of Section 215 orders in 2008).

** *See* U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS 37, 120 (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf (number of NSL requests in 2000 through 2005); U.S. 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, 107 (Mar. 2008), *available at* http://www.usdoj.gov /oig/special/s0803b/final.pdf (number of NSL requests in 2006); Letter from Ronald Weich, Assistant Attorney General, U.S. Department of Justice, to Harry Reid, Majority Leader, U.S. Senate (May 14, 2009), *available at* http://www.fas.org/irp/agency/doj/fisa/2008rept.pdf (number of NSL requests in 2007 and 2008).

*** U.S. DEP'T OF THE TREASURY, FINANCIAL CRIMES ENFORCEMENT NETWORK, THE SAR ACTIVITY REVIEW – BY THE NUMBERS, ISSUE 12, 4 (June 2009), *available at* http://www.fincen.gov/news_room/rp/files/sar_by_numb_12.pdf.

Plainly, the majority of Americans who have now had the personal, financial information involuntarily turned over to the federal government through the voluntary actions of their banks have not been charged with any wrongdoing. But, these records will stay in the federal databases indefinitely. Even though the Senate Judiciary Committee does not have primary jurisdiction over FinCEN matters, it should explore how these powers relate to the demands for financial information with NSLs.

Financial records now represent a significant component of the FBI's data "warehouse," which reported having almost 1 billion records as of late 2008. That is three times more records than people in the U.S. As the Electronic Frontier Foundation has noted, that is more records than are held by the largest library in the world, the Library of Congress, which has "138 million items in its collection."[6] As Bart Gellman reported in 2005, the Investigative Data Warehouse only began five years ago, in 2004, and already it has accumulated a billion records. If the number of records contained in the IDW were compared to the pie chart on the prior page, the IDW pie would be 50 times larger. Yet, there has been almost no public examination or hearings focused on this gargantuan database. And the IDW is focused primarily on U.S. records and people in the U.S. The FBI has a whole separate data warehouse, the Foreign Terrorist Tracking Task Force (FTTTF) "Datamart," for foreign terrorism investigations focused abroad, and that database has even more records in it than the IDW.

Additionally, despite revelations by Mr. Gellman and others, there has been no public examination of how the FBI is using contracts it has with the databroker ChoicePoint or with LexisNexis' financial assets databases to obtain or verify and obtain information about Americans. It is certainly the case that the Executive Branch has elsewhere said that it is determined to exploit so-called "open source" data and that the government has a right to information that commercial companies have, but it is not clear precisely what rules the FBI is operating under when its agents access ChoicePoint, for example, or how this relates to compelling versus voluntary disclosures by traditional financial institutions under NSLs or 215 orders or other claimed authority. It is also not clear how much taxpayer money is going into these contracts and what meaningful privacy protections, if any, are being applied. There is no information about how much private companies may be profiting by selling access to this data to the federal government. And, there has been no reporting about how many Americans have had information about them that may have been accumulated by ChoicePoint accessed by the government. And, the public has a right to know the answers to these questions.

These issues may seem complicated on the surface, but they are really about a fundamental question in a democracy: how much information should the government be able to accumulate about a person, without any evidence of any wrongdoing. I would submit that the answer should be very little, but it seems the government thinks the answer should be almost unlimited. And, nowadays, there is no need to create a separate file on a particular person when all the data can easily be aggregated at the touch of a button through the use of internal search engines that can accumulate information about a person.

B. Section 206 and Related Secret Wiretapping Needed Reforms

Just as the discussion of Section 215 of the Patriot Act implicates other powers with broader impact on individual privacy, Section 206 cannot be reasonably understood without reference to FISA powers. Before news broke that President Bush violated federal laws requiring judicial approval to conduct electronic surveillance in the US in investigations to prevent terrorism, he misled the American people,

[6] http://www.eff.org/issues/foia/investigative-data-warehouse-report. For a comprehensive examination of the IDW, access EFF's report.

telling Marylanders and Ohioans in 2005 that the government "needs a federal judge's permission to wiretap a foreign terrorist's phone, a federal judge's permission to track his calls . . . ." Back in 2004, in an effort to blunt controversy about his powers, President Bush assured New Yorkers: "Any time you hear the United States government talking about a wiretap, it requires—a wiretap requires a court order. Nothing has changed, by the way. When we're talking about chasing down terrorists, we're talking about getting a court order before we do so."

Once Eric Lichtblau and James Risen of the New York Times broke the story about the extraordinary electronic surveillance the administration was engaging in without warrants and in violation of the law, President Bush and his aides claimed that he was not misleading because he was talking about the Patriot Act's roving wiretap provisions. But, that was just more misinformation. The false implication was that the Patriot Act was totally separate from the laws the administration had broken. The Patriot Act amended the law President Bush broke but did not repeal the requirement of individualized judicial warrants for terrorism wiretaps.

Indeed, before the story broke, even the President's own advisors used to concede: "the primary provision in the Patriot Act makes amendments to the Foreign Intelligence Surveillance Act [FISA], which is the secret court you hear about that issues secret wiretaps. . . for over 25 years that have been tested in the courts that strike the proper balance between expanding our fight against terrorism, but protecting civil liberties at the same time." This is what John Yoo, former Bush appointee in DOJ's Office of Legal Counsel, told this to CNN in 2005. Yet, Mr. Yoo knew the administration was not following these rules because Mr. Yoo helped write the memos that rationalized evading the very requirements he was extolling on national television.

The suggestion that these binding laws somehow do not apply to terrorism ignores the plain language of the laws that were broken. It is important to recall that the Bush Administration asked for, and Congress passed, several amendments to the electronic surveillance provisions of FISA in the Patriot Act, which is titled "Providing Appropriate Tools Required to Intercept and Obstruct Terrorism." And FISA expressly constituted the "exclusive" rules for foreign intelligence surveillance in the US, including electronic surveillance to prevent "international terrorism," making it a crime to wiretap without court approval.

Under classic FISA, it does not matter whether the wiretaps involve multiple phones, known as multi-point or "roving" wiretaps, or involve just one phone. Federal law requires judicial approval for all electronic surveillance of Americans. To accept the assertions would require accepting the false claim that the only time judges are required is when the person tapped is using more than one phone. The law required individual warrants no matter how few or how many phones or email accounts are tapped.

Until last year, FISA required that the government identify the telephone or device to be tapped in a secret wiretap order. But, with last year's passage of the FISA Amendments Act (FAA), the government is not required to disclose to the court the "facility" where the acquisition of electronic information takes place, let alone particular phones, for surveillance that meets the FAA's test. So, the Section 206 rules that permit what have become known as "John Doe roving wiretaps" apply to a narrow category of cases within the U.S. that are not covered by the broad orders for electronic surveillance of international communications that are permitted under the FAA, orders that I and others believe are unconstitutional. That is why I support not just Senator Feingold's amendments to cure the flaws in the roving wiretap powers, but also the much needed changes he proposes to the revised FISA authorities. I support Senator Feingold's amendments in Title III of his bill to address these issues.

9

The amendment against bulk collection is particularly important because of the way the FISA Amendments Act could be construed and especially in light of the "over-collection" revelations earlier this year. Additionally, I know that the FISA Amendments Act attempted to bar using blanket orders for electronic collection from being used to acquire purely domestic communications. However, President Bush and his allies inserted language in the bill making the bar on collecting domestic calls or e-mails applicable only when the government knows "at the time of acquisition" that the sender and all recipients are physically located in the U.S. This weasel language permits ignorance to be bliss when it comes to rules intended to protect purely domestic calls or emails. The other amendments in Title III are also important and would help restore civil liberties in this country.

Even though there is little political appetite to revisit the FISA rules, I think doing so is important in the context of the Patriot reauthorization debate. For example, the public has never received a clear answer about the published reports that FBI agents were distracted by ineffective and wasteful surveillance leads generated from the NSA's illegal electronic surveillance program.[7] Here is part of that report:

> In the anxious months after the Sept. 11 attacks, the National Security Agency began sending a steady stream of telephone numbers, e-mail addresses and names to the F.B.I. in search of terrorists. The stream soon became a flood, requiring hundreds of agents to check out thousands of tips a month. But virtually all of them, current and former officials say, led to dead ends or innocent Americans. . . . "We'd chase a number, find it's a school teacher with no indication they've ever been involved in international terrorism - case closed," said one former FBI official, who was aware of the program and the data it generated for the bureau. "After you get a thousand numbers and not one is turning up anything, you get some frustration."

As Suzanne Spaulding has previously suggested, and Kate Martin and I have repeatedly urged, we need a comprehensive examination of the domestic surveillance authorities and uses. Until this kind of far-ranging review is complete, the American people will be stuck with a patchwork of authorities that serve neither liberty nor security well.

C. Other Powers in Need of Reform

In addition to these powers, I would urge Congress to take a closer look at Section 213 of the Patriot Act, which granted sneak and peek powers in routine criminal cases, overwhelmingly in cases that have nothing to do with terrorism. I would also urge that the Committee take another look at the so-called "lone wolf" provision, which has reportedly not be used by the government, as well as other provisions addressed in Senator Feingold's set of amendments.

I would also like to commend Senator Leahy again for the base bill he has introduced on this issue, and all he has done and continues to do to defend individual rights and support common-sense improvements to the law. I understand that there is precious little time to resolve all these issues before the end of this Session of Congress, but I urge that these issues be examined and be resolved publicly to the extent possible.

Thank you again for the invitation and for considering my views.

---

7 Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta Jr., "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," THE NEW YORK TIMES (January 17, 2006).

Department of Justice

STATEMENT OF

DAVID KRIS
ASSISTANT ATTORNEY GENERAL

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ENTITLED

"REAUTHORIZING THE USA PATRIOT ACT:
ENSURING LIBERTY AND SECURITY"

PRESENTED

SEPTEMBER 23, 2009

Statement of
David Kris
Assistant Attorney General
Before the
Committee on the Judiciary
United States Senate
For a Hearing Entitled
"Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security"
Presented
September 23, 2009

Chairman Leahy, Ranking Member Sessions, and Members of the Senate Judiciary Committee, thank you for inviting me to speak to you today about the Administration's position regarding three Patriot Act Provisions that will, by their terms, expire on December 31, 2009. We believe that the best legislation will emerge from a careful and collaborative examination of these matters. As you know, today's hearing has been preceded by extensive discussion and deliberation within the legislative and executive branches, and constructive discussions have recently begun between Administration officials and Congressional staff. I would like to extend the Attorney General's gratitude for providing the Department with this opportunity to present the Administration's views formally to the Members of this Committee today.

Before I address each of the three expiring authorities, I would like to address a concern raised often during our discussions with Committee staff. The Department understands that Members of Congress may propose modifications to the legislation governing the three expiring authorities and other related authorities with the goal of providing additional protection for the privacy of law abiding Americans. The protection of privacy and civil liberties is of deep and abiding concern to the Department of Justice, and to the Administration as a whole. We are ready and willing to work with Members on any specific proposals you may have to craft legislation that both provides effective investigative authorities and protects privacy and civil liberties.

With respect to the three expiring authorities, we recommend reauthorizing section 206 of the USA PATRIOT Act, which provides for roving surveillance of targets who take measures to thwart FISA surveillance. It has proven to be an important intelligence-gathering tool in a small but significant subset of FISA electronic surveillance orders.

This provision states that where the Government sets forth in its application for a surveillance order "specific facts" indicating that the actions of the target of the order "may have the effect of thwarting" the identification, at the time of the application, of third parties necessary to accomplish the ordered surveillance, the order shall direct such third parties, when identified, to furnish the Government with all assistance necessary to accomplish surveillance of the target identified in the order. In other words, the "roving" authority is only available when the Government is able to provide specific information that the target may engage in counter-

surveillance activity (such as rapidly switching cell phone numbers). The language of the statute does not allow the Government to make a general, "boilerplate" allegation that the target may engage in such activities; rather, the Government must provide specific facts to support its allegation.

There are at least two scenarios in which the Government's ability to obtain a roving wiretap may be critical to effective surveillance of a target. The first is where the surveillance targets a traditional foreign intelligence officer. In these cases, the Government often has years of experience maintaining surveillance of officers of a particular foreign intelligence service who are posted to locations within the United States. The FBI will have extensive information documenting the tactics and tradecraft practiced by officers of the particular intelligence service, and may even have information about the training provided to those officers in their home country. Under these circumstances, the Government can furnish specific facts in its application to the FISA Court that demonstrate that the actions of the individual may have the effect of thwarting the identification of third parties whose assistance is needed to conduct the surveillance.

The second scenario in which the ability to obtain a roving wiretap may be critical to effective surveillance is the case of an individual who actually has engaged in counter-surveillance activities or in preparations for such activities. In some cases, individuals already subject to FISA surveillance are observed to be engaging in counter-surveillance or instructing associates on how to communicate with them through more secure means. In other cases, non-FISA investigative techniques have revealed counter-surveillance preparations (such as buying "throwaway" cell phones or multiple calling cards). The Government then offers these specific facts to the FISA court as justification for a grant of roving authority.

Since the roving authority was added to FISA in 2001, the Government has sought to use it in a relatively small number of cases (on average, twenty-two applications annually for 2003-2008). We would be pleased to brief Members or staff regarding specific case examples in a classified setting. The FBI uses the granted authority only when the target actually begins to engage in counter-surveillance activity that thwarts the already-authorized surveillance, and does so in a way that renders the use of roving authority feasible.

Roving authority is subject to the same court-approved minimization rules that govern other electronic surveillance under FISA and that protect against the acquisition or retention of non-pertinent information. The statute generally requires the Government to notify the FISA court within 10 days of the date upon which surveillance begins to be directed at any new facility. Over the past seven years, this process has functioned well and has provided effective oversight for this investigative technique.

We believe that the basic justification offered to Congress in 2001 for the roving authority remains valid today. Specifically, the ease with which individuals can rapidly shift between communications providers, and the proliferation of both those providers and the services they offer, almost certainly will increase as technology continues to develop.

International terrorists, foreign intelligence officers, and espionage suspects — like ordinary criminals — have learned to use these numerous and diverse communications options to their advantage. Any effective surveillance mechanism must incorporate the ability to address rapidly an unanticipated change in the target's communications behavior. The roving electronic surveillance provision has functioned as intended and has addressed an investigative requirement that will continue to be critical to national security operations. Accordingly, we recommend reauthorizing this feature of FISA.

We also recommend reauthorizing section 215 of the USA PATRIOT Act, which allows the FISA court to compel the production of "business records." The business records provision addressed a gap in intelligence collection authorities that had previously existed and has proven valuable in a number of contexts.

The USA PATRIOT Act made the FISA authority relating to business records roughly analogous to that available to FBI agents investigating criminal matters through the use of grand jury subpoenas. The original FISA language, added in 1998, limited the business records authority to four specific types of records, and required the Government to demonstrate "specific and articulable facts" supporting a reason to believe that the person to whom the requested records pertain was a foreign power or an agent of a foreign power. In the USA PATRIOT Act, the authority was changed to encompass the production of "any tangible things" and the legal standard was changed to relevance to an authorized investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

The Government first used the USA PATRIOT Act business records authority in 2004 after extensive internal discussions over its proper implementation. The Department's inspector general evaluated the Department's implementation of this new authority at length, in reports that are now publicly available. Other parts of the USA PATRIOT Act, specifically those eliminating the "wall" separating intelligence operations and criminal investigations, also had an effect on the operational environment. The greater access that intelligence investigators now have to criminal tools (such as grand jury subpoenas) reduces but does not eliminate the need for intelligence tools, such as the business records authority. The operational security requirements of most intelligence investigations still require the secrecy afforded by the FISA authority.

For the period 2004-2008, the FISA court has issued about 236 orders to produce business records. Of these, 173 orders were issued in 2004-06 in combination with FISA pen register orders to address an anomaly in the statutory language that prevented the acquisition of subscriber identification information ordinarily associated with pen register information. Congress corrected this deficiency in the pen register provision in 2006 with language in the USA PATRIOT Improvement and Reauthorization Act. Thus, this use of the business records authority became unnecessary.

The remaining business records orders issued between 2004 and 2007 were used to obtain transactional information. As many Members are aware, some of these orders were used

to support important and highly sensitive intelligence collections. The Department can provide additional information to Members or their staff in a classified setting.

It is noteworthy that no recipient of a FISA business records order has ever challenged the validity of the order, despite the availability, since 2006, of a clear statutory mechanism to do so. At the time of the USA PATRIOT Act, there was concern that the FBI would exploit the broad scope of the business records authority to collect sensitive personal information on constitutionally protected activities, such as the use of public libraries. This simply has not occurred, even in the environment of heightened terrorist threat activity. The oversight provided by Congress since 2001, the specific oversight provisions added to the statute in 2006, and the requirement that the government make a specific showing to the FISA Court in each application have helped to ensure that the authority is being used as intended.

Based upon this operational experience, we believe that the FISA business records authority should be reauthorized. There will continue to be instances in which FBI investigators need to obtain transactional information that does not fall within the scope of authorities relating to national security letters and are operating in an environment that precludes the use of less secure criminal authorities. Moreover, in some instances, such as counterintelligence investigations, the use of criminal authorities may be inappropriate because the investigation is not focused on a violation of criminal law. Many of these instances will be mundane (as they have been in the past), such as the need to obtain driver's license information that is protected by State law. Others will be more complex, such as the need to track the activities of intelligence officers through their use of certain business services. In all these cases, the availability of a generic, court-supervised FISA business records authority is the best option for advancing national security investigations in a manner that protects privacy and civil liberties. The absence of such an authority could force the FBI to sacrifice key intelligence opportunities, to the detriment of the national security.

Finally, the Department recommends reauthorizing Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004, which defines a "lone wolf" agent of a foreign power and allows a non-United States person who "engages in international terrorism activities" to be considered an agent of a foreign power under FISA.

Enacted in 2004, this provision arose from discussions inspired by the Zacarias Moussaoui case. The basic idea behind the authority was to cover situations in which information linking the target of an investigation to an international group was absent or insufficient, although the target's engagement in "international terrorism" was sufficiently established. The definition is quite narrow: it applies only to non-United States persons; the activities of the person must meet the FISA definition of "international terrorism"; and the information likely to be obtained must be foreign intelligence information. What this means, in practice, is that the Government must know a great deal about the target, including the target's purpose and plans for terrorist activity (in order to satisfy the definition of "international terrorism"), but still be unable to connect the individual to any group that meets the FISA definition of a foreign power.

To date, the Government has not encountered a case in which this definition was both necessary and available, *i.e.*, the target was a non-United States person. Thus, the definition has never been used in a FISA application. We do not believe, however, that this means the authority is now unnecessary. Subsection 101(b) of FISA provides ten separate definitions for the term "agent of a foreign power" (five applicable only to non-United States persons, and five applicable to all persons). Some of these definitions cover the most common fact patterns; others describe narrow categories that may be encountered rarely. Although the latter group may be rarely encountered, it includes legitimate targets that cannot be accommodated under the more generic definitions and will escape surveillance but for the more specific definitions.

We believe that the "lone wolf" provision falls squarely within this class. While we cannot predict the frequency with which it may be used, we can foresee situations in which it would be the only avenue to effect surveillance. For example, we could have a case in which a known international terrorist affirmatively severs his connection with his group, perhaps following some internal dispute. Although the target still would be an international terrorist and an appropriate target for intelligence surveillance, the Government could no longer represent to the FISA court that he is currently a member of an international terrorist group or acting on its behalf. In the absence of the "lone wolf" definition, the Government would have to postpone FISA surveillance unless and until the target could be linked to another group. The absence of a known connection would not, however, necessarily mean that the individual did not pose a real and imminent threat. The lone wolf provision may also be required to conduct surveillance on an individual who "self-radicalizes" by means of information and training provided via the Internet. Although this target would have adopted the aims and means of international terrorism (and therefore be a legitimate national security target), he would not actually be acting as an agent of a terrorist group. Without the lone wolf definition, the Government might be unable to establish FISA surveillance.

These scenarios are not remote hypotheticals; they are based on trends we observe in current intelligence reporting. We cannot determine how common these fact patterns will be in the future or whether any of the targets will so completely lack connections to groups that they cannot be accommodated under other definitions. The continued availability of the lone wolf definition eliminates any gap. The statutory language of the existing provision ensures its narrow application, so the availability of this potentially useful tool carries little risk of overuse. We believe that it is essential to have the tool available for what we believe will be the rare situation in which it is necessary rather than to delay surveillance of a terrorist in the hopes that the necessary links are established or even to forego it entirely because such links cannot be established.

In short, the Department and the Administration believe that each of these three provisions provides important and effective investigative authorities. We believe that the current statutory scheme, together with the rules, guidelines, and oversight mechanisms observed by the Executive branch with respect to these authorities, safeguard Americans' privacy and civil liberties. We look forward to working with the Committee to reauthorize these important authorities in a manner that continues to protect both national security and privacy and civil liberties.

Statement Of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Judiciary Committee,
On "Reauthorizing The USA PATRIOT Act: Ensuring Liberty And Security"
September 23, 2009

After September 11, I worked to ensure that the USA PATRIOT Act ("Patriot Act") included oversight to make certain that the increased information-gathering powers of the Government, which could sweep in U.S. citizens, would be implemented appropriately. Working with then House Majority Leader, Republican Dick Armey, we included sunsets for some of the provisions with the greatest potential to directly affect Americans.

We debated the reauthorization of the Patriot Act for several months in 2005 and 2006. I again worked to protect the civil liberties and constitutional rights of Americans while providing the Government with the tools it needs to aggressively pursue those who would do us harm. Unfortunately, the reauthorization bill of 2006 lacked sufficient constitutional protections against the vast authorities it granted to the Government. I worked with Senator Specter to expand public transparency and congressional oversight, and included new sunsets in that bill. In the end, however, several important checks and balances were not included in the final version, and so I voted against it.

With three provisions expiring on December 31, 2009, we have an opportunity to consider the Patriot Act once again. We have another chance to get it right. The provisions slated to expire at the end of this year include the authorization for roving wiretaps, the "lone wolf" measure, and orders for tangible things, commonly referred to as Section 215 of the 2001 Patriot Act, or the "library records" provision.

In March, I sent a letter to Attorney General Holder requesting the administration's views on these expiring provisions. I reiterated that request at a Judiciary Committee oversight hearing in June. I recently received a letter from the Department of Justice urging Congress to extend the expiring authorities, but also noting the President's and the Attorney General's emphasis on accountability and checks and balances, and their willingness to consider additional ideas. That openness is a welcome change from the previous administration, and I look forward to exploring it today.

Yesterday, I introduced a bill with Senators Cardin and Kaufman that aims to strike the kind of balance the administration urges. It will extend the authorization of the three expiring provisions with new sunsets. It adds checks and balances by increasing judicial review of Government powers that capture information on U.S. citizens. It expands congressional oversight and public reporting on the use of intrusive surveillance measures. The Leahy-Cardin-Kaufman bill mandates new audits by the Department of Justice Office of Inspector General on the use of Section 215 orders and NSLs. We all appreciate the earlier audits conducted by Inspector General Glenn Fine and the improvements to which they have led. In developing our proposal, I have consulted with Senators Feingold and Durbin, who introduced a more expansive bill last week, and, with their encouragement, borrowed a few accountability provisions from their proposal. I have also shared early drafts of our proposal with Senator Feinstein, the chair of the Select Committee on Intelligence.

I have long been concerned over the issuance and oversight of National Security Letters (NSLs). They do not require approval by a court, grand jury, or prosecutor. They are issued in secret, with recipients silenced, under penalty of law. Yet NSLs allow the Government to collect sensitive information, such as personal financial records. As Congress expanded the NSL authority in recent years, I raised concerns about how the FBI handles the information it collects on Americans with no real limits imposed by Congress. We now know that the NSL authority was significantly misused. In 2008 Inspector General Fine issued a report on the FBI's use of NSLs revealing serious over-collection of information and abuse of the NSL authority.

In response to these concerns, our bill would impose higher standards on the issuance of NSLs and improve judicial oversight of their use. The bill also addresses the constitutional deficiency recently identified by the Second Circuit Court of Appeals, which found that the nondisclosure, or "gag orders," issued under NSLs infringe constitutional rights, as I have long maintained. The bill establishes a procedure giving the recipient of an NSL greater ability to challenge a gag order, eliminates presumptions that allow the Government to ensure itself of victory in defending such orders, and imposes a renewable one-year time limit on these orders.

The Leahy-Cardin-Kaufman bill also adds a sunset on NSLs, to guarantee that Congress will continue to examine the use of this authority. I introduced a bill in 2006, after the most recent Patriot Act reauthorization, to impose a sunset on NSLs. This sunset provision, combined with comprehensive audits, will help to hold the FBI accountable in its use of this authority.

The power of the Government to collect records for tangible things under Section 215 of the original Patriot Act, commonly referred to as the "library records" provision, is another authority that I fought hard to reform during the last reauthorization. The Leahy-Cardin-Kaufman bill adopts the appropriate constitutional standard that I supported in 2006. The standard we propose eliminates the presumption in favor of the Government and, instead, requires the Government to show the connection between the items sought and a suspected terrorist or spy.

This bill would also establish more meaningful judicial review of Section 215 orders and the gag orders covering them. It repeals the requirement in current law that requires a recipient of a Section 215 nondisclosure order to wait for a full year before challenging that gag order. It also repeals the conclusive presumption in favor of the Government for such gag orders any time a high-level official certifies that disclosure of the order would endanger national security or interfere with diplomatic relations. These restraints on meaningful judicial review are unfair, unjustified, and completely unacceptable. I fought hard to keep these two provisions out of the 2006 reauthorization, but the Republican majority at that time insisted they be included.

The Leahy-Cardin-Kaufman bill also improves Government accountability through more transparent public reporting of the use of surveillance, and by requiring audits of how these vast authorities have been used since they were last reauthorized. At the insistence of several of us in the Senate, the 2006 reauthorization bill required reviews by the Justice Department's Inspector General of the use of Section 215 orders and NSLs. The Inspector General audits produced vital information about misuse, weak data collection, and a host of other problems associated with the implementation of surveillance laws. FBI Director Mueller agreed with me at our oversight hearing last week that the Inspector General audits helped the FBI to improve procedures and

curb abuses and that outside oversight was essential. I look forward to hearing from Inspector General Glenn Fine about the lessons he has learned from those reviews and about the importance of continued oversight.

This bill will strengthen court oversight of Section 215 orders by requiring court oversight of minimization procedures when information concerning a U.S. person is acquired, retained, or disseminated. Requiring FISA Court approval of minimization procedures would simply bring Section 215 orders in line with other FISA authorities -- such as wiretaps, physical searches, and pen register and trap and trace devices -- that already require FISA court approval of minimization procedures. This is another common sense modification to the law that was drafted in consultation with Senators Feingold and Durbin. If we are to allow personal information to be collected in secret, the court must be more involved in making sure the authorities are used responsibly and that Americans' information and personal privacy are protected.

Finally, this bill addresses concerns over the use of pen register or trap and trace devices ("pen/trap"). The bill raises the standard for pen/trap in the same manner as it raises the standard for Section 215 orders. The Government would be required to show that the information it seeks is both relevant to an investigation and connected to a suspected terrorist or spy. This section also requires court review of minimization procedures, which are not required under current law, and adds an Inspector General audit of the use of pen/trap that is modeled on the audits of Section 215 orders and NSLs.

I look forward to hearing from this distinguished panel of witnesses, and to working with the members of this Committee as we consider the important issues this reauthorization raises. We have no time to delay. I hope to turn to the issue at our Committee meeting on October 1, a week from tomorrow.

#####

Hearing on the USA PATRIOT Act

Committee on the Judiciary

United States Senate

Wednesday, September 23, 2009

Testimony
of
Suzanne E. Spaulding, Esq.

Subcommittee on the Constitution, Civil Rights, and Civil Liberties

Judiciary Committee

United States House of Representatives

Hearing on the USA PATRIOT Act

Wednesday, September 23, 2009

Testimony
of
Suzanne E. Spaulding, Esq.

Chairman Leahy, Ranking Member Sessions, and members of the Committee, thank you for inviting me to participate in today's hearing on the USA PATRIOT Act and related provisions. Four years ago, I testified in Congress regarding the provisions of the PATRIOT Act that were designated to sunset in 2005. A number of

concerns with the original language in the Act were addressed in the Reauthorization Act of 2006. However, some remain, particularly some of the overarching issues, and some were compounded in subsequent legislation.

As I attempt to address these issues this morning, I am mindful that we recently marked another anniversary of the attacks of September 11, 2001. This indelible manifestation of the terrorist threat continues to fuel our determination to ensure that those in our government who work so tirelessly to protect us from another attack have the tools they need and that we are not undermining their efforts by failing to consider strategic as well as tactical objectives. In the eight years since 9/11, we have learned a great deal about the nature of the terrorist threat and the best ways to combat it. Armed with that wisdom, and with determination rather than fear, it is appropriate--and important for our national security-- that we continue to reexamine our response.

We have to demonstrate that we still believe what our founders understood; that respect for civil liberties is not a luxury of peace and tranquility. Instead, in a time of great peril, it was seen as the best hope for keeping this nation strong and resilient. The men who signed the Constitution and those who developed the Bill of Rights were not fuzzy-headed idealists but individuals who had fought a war and knew that they faced an uncertain and dangerous time. Respect for the Constitution and careful efforts to ensure that our laws protect the rights enshrined therein are a source of strength and can be a powerful antidote to the twisted lure of the terrorist's narrative. In fact, after spending nearly 20 years working terrorism issues for the government, I am convinced that this approach is essential to defeating the terrorist threat.

With this understanding of the national security imperative, I support this committee's intention not to limit its review to those few provisions that are scheduled to sunset. Instead, Congress should use this opportunity to examine ways to improve other domestic intelligence laws as well, such as the various provisions for national security letters. As I have urged before, Congress should undertake a comprehensive review of domestic intelligence activities, and I would encourage the Administration to do the same.

The legal framework for domestic intelligence has come to resemble a Rube Goldberg contraption rather than the coherent foundation we expect and need from our laws. The rules that govern domestic intelligence collection are scattered throughout the US Code and in a multitude of internal agency policies, guidelines, and directives, developed piecemeal over time, often adopted quickly in response to scandal or crisis and sometimes in secret. They do not always reflect a firm understanding of why intelligence collection needs to be treated differently than law enforcement investigations, the unique intelligence requirements for homeland security, the impact of dramatic changes in technology, and the degree to which respect for civil liberties, fundamental fairness, and the rule of law is essential to winning the battle for hearts and minds--and, therefore, essential to our homeland security.

The various authorities for gathering information inside the United States, including the authorities in FISA, need to be considered and understood in relation to each other, not in isolation. For example, Congress needs to understand how FISA surveillance authority relates to current authorities for obtaining or reviewing records, such as national security letters, Section 215, the physical search and pen register/trap and trace authorities in FISA, and the counterparts to these in the criminal context, as well as other law enforcement tools such as grand juries and material witness statutes.[1]

Executive Order 12333, echoed in FISA, calls for using the "least intrusive collection techniques feasible." The appropriateness of using electronic surveillance or other intrusive techniques to gather the communications of Americans should be considered in light of other, less intrusive techniques that might be available to establish, for example, whether a phone number belongs to a suspected terrorist or the pizza delivery shop. Electronic surveillance is not the "all or nothing" proposition often portrayed in some of the debates.

In addition, President Obama has already committed to asking his Attorney General to conduct a comprehensive review of domestic surveillance. If that review is not already underway, Congress should encourage its initiation. The IG Report on the Terrorist Surveillance Program clearly indicated that there were programs beyond its scope. These need to be examined and a report made to Congress and, to the maximum extent possible, to the public.

I understand that today's hearing, however, is particularly focused on the provisions that will sunset at the end of this year, so the balance of my testimony will address those.

---

[1] See, for example, the May 2008 OIG Report on Section 215, which cites concerns about the FBI's use of NSLs to get information "after the FISA Court, citing First Amendment concerns, had twice declined to sign Section 215 orders in the same investigation." The IG questioned the appropriateness of this "because NSLs have the same First Amendment caveat as Section 215 requests and the FBI issued the NSLs based on the same factual predicate, without further reviewing the underlying investigation to ensure that it was not premised solely on protected First Amendment conduct." OIG Report at 5.

Distinguishing between domestic intelligence operations and criminal law enforcement investigations

Sections 215 and 206 of the PATRIOT Act, like most domestic intelligence authorities, both have corollaries in the criminal context. This was often cited as justification for providing for these authorities in the intelligence context: "if we can do these kinds of things when investigating drug dealers, certainly we should have this authority for intelligence operations against terrorists." It's a compelling argument. But sometimes important elements get lost in the translation from the criminal to intelligence realm.

Intelligence operations are often *wide-ranging* rather than specifically focused—creating a greater likelihood that they will include information about ordinary, law-abiding citizens; they are conducted in *secret*, which means abuses and mistakes may never be uncovered; and they *lack safeguards* against abuse that are present in the criminal context where inappropriate behavior by the government could jeopardize a prosecution. These differences between intelligence and law enforcement help explain this nation's long-standing discomfort with the idea of a domestic intelligence agency.

Because the safeguards against overreaching or abuse are weaker in intelligence operations than they are in criminal investigations, powers granted for intelligence investigations should be no broader or more inclusive than is absolutely necessary to meet the national security imperative and should be accompanied by rigorous oversight within the executive branch, by Congress and, where appropriate, in the courts.

Unfortunately, this essential caution was often ignored in the FISA amendments contained in the PATRIOT Act. The authority actually became *broader* as it moved into the intelligence context and oversight was not always accordingly enhanced.

Section 206: Roving Wiretaps

Section 206 was intended to bring the roving wiretap authority that is available in criminal investigations into the realm of intelligence surveillance under FISA. This was an essential update but some important safeguards in the criminal provisions were lost in the transition.

In a criminal investigation, under Title III, roving wiretap applications must definitively identify the target of the surveillance. FISA roving wiretaps need only provide "a description of the target" if the identity is not known. This less rigorous standard increases the prospect that the government may wind up mistakenly intercepting communications of innocent persons.

In addition, Title III permits surveillance only when it is reasonable to assume that the suspect is "reasonably proximate" to the instrument that is being tapped--and only one instrument can be tapped at a time. This requirement, like the requirement to identify the target, was designed to reduce the likelihood that communications of innocent persons would be intercepted. This requirement is not in section 206.

Title III also differs from the FISA roving wiretap in requiring that the target be notified of the surveillance, generally 90 days after the surveillance ends. This notice requirement is understandably absent in the intelligence context but so, too, is the safeguard that notice provides as a mechanism to deter and detect mistakes or abuses.

Deterrence is also weakened in the intelligence context because prosecution is usually not the goal. In the criminal context, where the focus is on successful prosecution, the exclusionary rule serves an essential function, one that is largely absent in intelligence operations. As the Supreme Court explained in *Terry v. Ohio*, 392 U.S. 1 (1968):

> Ever since its inception, the rule excluding evidence seized in violation of the Fourth Amendment has been recognized as a principal mode of discouraging

> lawless police conduct. *See Weeks v. United States,* 232 U.S. 383, 391-393 (1914). Thus, its major thrust is a deterrent one, *see Linkletter v. Walker,* 381 U.S. 618, 629-635 (1965), and experience has taught that it is the only effective deterrent to police misconduct in the criminal context, and that, without it, the constitutional guarantee against unreasonable searches and seizures would be a mere "form of words." *Mapp v. Ohio,* 367 U.S. 643, 655 (1961).
>
> ...
>
> Regardless of how effective the rule may be where obtaining convictions is an important objective of the police, it is powerless to deter invasions of constitutionally guaranteed rights where the police either have no interest in prosecuting or are willing to forgo successful prosecution in the interest of serving some other goal.

Combine this with a statutory standard that is less rigorous than the criminal standard, both as regards the identity of the target and the proximity to the instrument, and you compound the risk of mistake or abuse. This highlights the care that must be taken when importing criminal authorities into the intelligence context, and why it may be necessary to include more rigorous standards and/or other safeguards.

For example, Congress should consider tightening the language to require the judge to determine that the target has been described with sufficient particularity to distinguish him or her from other potential users of the instrument or facility being surveilled.

Similarly, while it is possible that the proximity requirement is somehow included in the minimization procedures that are called for in section 206, Congress may want to consider explicitly including this requirement in the statute, as it is in Title III.

Finally, perhaps the FISA judge should have the discretion to impose a time limit on the lack of notice, giving the government an opportunity to argue for an extension if circumstances warrant it.

Section 215: Tangible Things Orders

Section 215 of FISA also imported into the intelligence realm authority similar to that traditionally exercised in criminal investigations, in this case attempting to mimic the use of grand jury or administrative subpoenas.

However, the criminal investigative tools require some criminal nexus. Not necessarily that a crime has already been committed, but that the activity that is being investigated would violate a criminal statute. Under our constitution, criminal activity must be well defined so that individuals are clearly on notice with regard to whether their actions may violate the law and thus invite government scrutiny.

When the authority moved into the intelligence context, however, the requirement for a criminal nexus was dropped. Instead, section 215 orders require only that the information demanded by the government is "relevant to an authorized investigation (other than a threat assessment) ... to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities"

Consider this language. It does not say "an investigation into international terrorism activities"—which would at least mean there was some specific international terrorism activity being investigated. Instead, it says "an investigation *to protect against* international terrorism." This very broad language may or may not involve criminal activity and provides potentially far greater flexibility than criminal subpoenas. Again, this may be appropriate for the wide-ranging nature of intelligence collection-- but it also provides greater opportunity for abuse and mistakes. Amending the language to read "an investigation of international terrorism activities" should meet the national security imperative and provide better protection for innocent persons.

The Reauthorization Act of 2006 attempted to address this concern by adding a provision that the things being sought are "presumptively relevant to an authorized investigation if the applicant shows in the statement of the facts that they pertain to **(i)** a foreign power or an agent of a foreign power; **(ii)** the activities of a suspected agent of a

foreign power who is the subject of such authorized investigation; or **(iii)** an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation."[2]

The impact of this added language is not entirely clear. First, the third category, which includes anyone "known to" a suspected agent of a foreign power, is extremely broad and clearly could include completely innocent Americans. David Kris and Doug Wilson cite the example of the bank records of a grade-school teacher of the child of a suspected agent of a foreign power.[3] But it could also apply to your daughter's diary if she is in that child's class and known to the parent.

Moreover, this provision does not preclude the issuance of orders pursuant to facts that do not fall within any of these three categories. In other words, this language, by creating a presumption rather than a requirement, does not restrict the extremely broad scope of the term "relevant to" an investigation.

The weak safeguard provided by the "presumptively relevant" language also stems from the context in which Section 215 orders are considered. Creating a "presumption" generally implies a shift in the burden of proof from one party to another in an adversarial proceeding. Section 215 orders are considered in an ex parte proceeding, not in an adversarial context. Once served, an order can be challenged by the recipient but, if served on a third-party record holder, there is very little incentive for that record holder to challenge the order. In fact, the letter from the Department of Justice concedes that "no recipient of a FISA business records order has ever challenged the validity of the order." These record holders cannot be considered as fully representing the interests of the individual whose records are being sought.

---

[2] 50 USC 1861(b)(2).

[3] *National Security Investigations & Prosecutions*, David S. Kris and J. Douglas Wilson, Thomson West (2007) at 18:3.

Congress should consider changing the language to remove the presumption and make it clear that the tangible things being sought must be relevant to an authorized investigation *and* fall into one of these three categories.

The Reauthorization Act also added a requirement that the Section 215 application include "*a statement of facts* showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation." (Emphasis added.) The requirement to provide facts to back up the government's assertion was an improvement over the PATRIOT Act language, but pre-PATRIOT Act language in this section required the government to provide "specific and articulable facts." This is the standard normally used[4] and should be restored. The "specific and articulable" language may have been dropped in a mistaken belief that Section 215 does not implicate Fourth Amendment or other constitutional concerns. While this argument may have carried weight before the PATRIOT Act changes, it is certainly not valid today.

Section 215 as originally adopted by Congress in 1998 applied only to "records" from "a common carrier, public accommodation facility, physical storage facility or vehicle rental facility." This was properly entitled the "Business Records" provision. The PATRIOT Act amendments now allow the orders to be issued to obtain "any tangible things" from any person. This could include your personal notes, your daughter's diary, or your computer.

Congress should change the title of this provision to "Access to tangible things," to more accurately reflect the broad scope of items now susceptible to such orders. It is certainly not limited to 3rd party records, for example. Thus, even if you accept as still valid the "3rd-party-record rule," a premise that needs serious re-evaluation in light of data aggregation/data mining technology, this section would still include things to which the Fourth Amendment clearly applies. Moreover, as the OIG Report concluded, Section 215

[4] See, e.g., *Terry v. Ohio*, 392 U.S. 1 (1968).

orders can also raise issues related to the Fifth and First Amendments. (See IG Report at 81.)

Finally, Section 215 also puts the burden on the recipient of order to challenge a gag order before the government even has to certify that there would be any harm from disclosure. Congress should consider requiring the government to set forth in the initial application the grounds upon which it believes disclosure will be harmful.[5] And the one-year time frame should apply to the duration of all gag orders, perhaps with the FISA judge having discretion to impose a shorter time frame, renewable indefinitely.

Lone Wolf

Four years ago I urged Congress to let the Lone Wolf provision sunset. I reiterate that plea today.

The Foreign Intelligence Surveillance Act (FISA) is an extremely important and extraordinary national security tool whose policy and constitutional justification is needlessly undermined by the Lone Wolf provision. The Administration's admission that they have never once used the authority seems to provide compelling evidence that it was not needed and is not an essential counterterrorism tool.

The common wisdom "if it ain't broke, don't fix it" was ignored when Congress enacted the "Lone Wolf" amendment to the Foreign Intelligence Surveillance Act (FISA), allowing its use against an individual acting totally alone, with no connection to any foreign power, so long as they are "engaged in international terrorism or activities in preparation therefor." Although the Lone Wolf provision is often referred to as the "Moussaoui fix," in fact, no "fix" was needed in the Moussaui case because it was not FISA's requirements that prevented the FBI from gaining access to his computer back in August of 2001. The problem was a misunderstanding of FISA. This conclusion is

[5] This would be consistent with the federal court decision that found national security letter gag orders that do not require the government to initiate judicial review of the order or provide facts to support its assertions of harm to be an unconstitutional infringement of the First Amendment. *Doe v. Muksasey*, 549 f3d 861 (2d cir. 2008).

supported by the findings of the Joint Congressional Intelligence Committee Inquiry into the 9/11 Attacks, an exhaustive Senate Judiciary Committee inquiry, and the 9/11 Commission.

In order to obtain a FISA order authorizing access to Moussaoui's computer, the FBI needed to show probable cause to believe that Moussaoui was acting "for or on behalf of a foreign power." A foreign power is defined to include a group engaged in international terrorism. There is no requirement that it be a "recognized" terrorist organization. Two people can be "a group engaged in international terrorism." (See *FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures, An Interim Report* by Senators Patrick Leahy, Charles Grassley, & Arlen Specter (February 2003) at p. 17.)

Moreover, the government does not have to "prove" the target's connection to a terrorist group. They must merely meet the "probable cause" standard, which, as the Judiciary Committee Report points out, does not mean "more likely than not" or "an over 51% chance," but "only the probability and not a prima facie showing." The Report concluded that "there appears to have been sufficient evidence in the possession of the FBI which satisfied the FISA requirements for the Moussaoui application" (p. 23). Thus, no "fix" was required to search Moussaoui's computer.

Even if the FBI had not been able to meet the relatively low "probable cause" standard for showing that Moussaoui was working with at least one other person, the FBI could very likely have obtained a criminal warrant to search Moussaoui's computer. They did not pursue that because they were concerned that doing so would preclude them from getting a FISA warrant later if they were turned down for the criminal warrant or ultimately did develop what they thought was sufficient information linking him to a terrorist group. This concern was based on the "primary purpose" test—viewed as precluding the use of FISA if the primary purpose was criminal prosecution rather than intelligence collection—which was subsequently changed in the USA PATRIOT Act. Now

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

The Department of Justice in its letter to the Congress last week stated that this Lone Wolf authority had never been used but argued that we should keep it in FISA just in case. The problem with this reasoning is that it comes at a high cost. In addition to being unnecessary, the Lone Wolf provision—by extending FISA's application to an individual acting entirely on their own-- undermines the policy and constitutional justification for the entire FISA statute.

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

The Congressional debate, and the court cases that informed and followed it, clearly reflect the sense that this limited and extraordinary exception from the normal criminal warrant requirements was justified only when dealing with foreign powers or their agents. In 2002, the FISA Court of Review (FISCR) cited the statute's purpose, "to protect the nation against terrorists and espionage threats directed by foreign powers," to conclude that FISA searches, while not clearly meeting "minimum Fourth Amendment warrant standards," are nevertheless reasonable.[6] In its more recent case upholding the constitutionality of the Protect America Act *as applied*, the FISC again relied upon the

[6] *In re Sealed Case*, 310 F.3rd 717 (Foreign Intel. Surv. Ct. Rev. 2002).

government's decision to apply the authority only to *foreign powers or agents of foreign powers* reasonably believed to be outside the US.[7]

Individuals acting entirely on their own simply do not implicate the level of foreign and military affairs that courts have found justify the use of this extraordinary foreign intelligence tool. The FISA exception to the Fourth Amendment warrant standards was not based simply on a foreign nexus; it did not apply to every non-US person whose potentially dangerous activity transcended US borders. It was specifically limited to activities involving foreign powers.

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

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

---

[7] *In re Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, No. 08-1, August 22, 2008.

While the Administration admits to never having used this provision, and concedes that they cannot determine "whether any of the targets will so completely lack connections to groups that they cannot be accommodated under other definitions," the letter from the Department of Justice offers a couple of hypotheticals to justify the "just in case" argument. Keep in mind, however, that even if FISA surveillance and secret search authority were not available, the government can still investigate and, at least in the case of the "known" terrorist, make an arrest. For example, the government can find out all the people with whom each of those individuals is communicating, get their credit card information to see where they are at various times through the day and what transactions they engage in, and put them under physical surveillance. Finally, if there is an urgent need to conduct electronic surveillance before any indicia can be gathered that the person is working with someone else, Title III is a viable option.

If the government can make a compelling case that these investigative tools are inadequate, Congress could consider allowing the government to use authorities in FISA other than the most intrusive authorities of electronic surveillance and physical search to investigate a suspected Lone Wolf. In this way, the government could use Section 215 (and pen register/trap & trace authority, which does not require that the target is an agent of a foreign power), with the attendant secrecy, in order to gather indicia that at least one other person is involved--at which point the electronic surveillance and physical search authorities would be available.

Congress should let the terrorism Lone Wolf provision sunset. By defining an individual acting totally alone, with no connection to any other individual, group, or government, as "an agent of a foreign power," Congress adopted the logic of Humpty Dumpty, who declared: "When I use a word, it means just what I choose it to mean." Unfortunately, this legislative legerdemain stretched the logic of this important statutory tool to a point that threatens its legitimacy. If its use against a true Lone Wolf is ever challenged in court, FISA, too, may have a great fall.

Expansion of Lone Wolf

Unfortunately, instead of repealing or fixing the Lone Wolf provision, Congress expanded it. The FISA Amendments Act enacted last year added to the "agent of a foreign power" definition a non-US person "engaged in the international proliferation of weapons of mass destruction." This not only repeats the error of targeting an individual acting alone, it compounds the concern by removing any requirement that the activity constitute a crime.

The definition of "international terrorism" at least includes a requirement that the activity "involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State." As noted in the discussion above regarding Sections 206 and 215, the requirement for a criminal predicate is significant because, in our system, individuals are held to be on notice, through the careful definitions in the criminal code, of when they are engaging in criminal activity and thereby risking government intrusion, such as electronic surveillance of their communications.

"International proliferation of weapons of mass destruction" is not defined in FISA. Instead, the amendments included a definition of "weapons of mass destruction." The activity that puts an individual at risk of government surveillance, however, is "proliferation" of those weapons. The innocent, unwitting sale of dual-use goods to a foreign front company could be considered proliferation. If so, a non-US person working for an American company who is involved in completely legal sales of such dual-use goods could have all of their communications monitored and their home secretly searched by the US government.

I served as the Legal Adviser for the intelligence community's Nonproliferation Center and as Executive Director of a Congressionally-created WMD commission, so I fully understand the imperative to stop the spread of these dangerous technologies.

However, there are many tools available to investigate these activities without permitting the most intrusive technique--listening to phone calls, reading emails, and secret physical searches--to be used against people who are unwittingly involved and whose activities are legal. This overly broad extension of FISA raises significant constitutional issues.

Congress should add a "knowing" requirement, just as there is for aiding and abeting clandestine intelligence activities. Alternatively, Congress should define "proliferation" to include only activity that would constitute a crime.

Conclusion

Let me close by commending the Committee for its commitment to ensuring that the government has all appropriate and necessary tools at its disposal in this vitally important effort to counter today's threats and that these authorities are crafted and implemented in a way that meet our strategic goals as well as tactical needs. With a new Administration that provokes less fear of the misuse of authority, it may be tempting to be less insistent upon statutory safeguards. On the contrary, this is precisely the time to seize the opportunity to work with the Administration to institutionalize appropriate safeguards in ways that will mitigate the prospect for abuse by future Administrations, or even this Administration in the wake of some event.

Thank you.

STATEMENT OF

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

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING

THE USA PATRIOT ACT SECTIONS 206 AND 215 AND THE "LONE WOLF" PROVISION OF THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

PRESENTED ON

SEPTEMBER 23, 2009

I. Introduction

Chairman Leahy, Ranking Member Sessions and Members of the Committee, thank you for the invitation to appear before you today. Thank you also for holding this important hearing and soliciting our thoughts about the Patriot Act and the three provisions that are scheduled to expire at the end of this year.

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 of this year, I served in a variety of capacities, including Homeland Security Advisor to the President, Assistant Attorney General for National Security at the Department of Justice, United States Attorney, General Counsel and Chief of Staff of the FBI and career federal prosecutor. I was honored to work for many years alongside the men and women who devote themselves to the protection of our country, and to participate in the policy and legislative response to the terrorist threat that became manifest on September 11, 2001. I have also been honored to participate -- along with my co-panelists -- in what has been a very constructive national discussion over the past eight years about the appropriate parameters of the government's investigative capabilities in our country's fight against international terrorism.

Today, I will discuss some of the investigative authorities that our government relies upon to protect our national security and, in particular, the three amendments to the Foreign Intelligence Surveillance Act (FISA) that are scheduled to expire at the end of this year absent reauthorization. It is my position that all three authorities -- the roving wiretap authority, the business records order provision and the authority to surveil a "lone wolf" international terrorist -- are important to our national security and should be reauthorized.

II. Background to the Reauthorization Decision

Before addressing these three specific provisions, however, it is useful to consider where we find ourselves today in the evolution of our national security authorities since September 11, 2001. Immediately after the attacks of that day, Congress took stock of our national security authorities and found them inadequate. They were 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 afford sufficient coordination and information sharing between law enforcement and intelligence professionals; 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 the 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.

With the memory of 9/11 fresh in their minds, Congress drew up an omnibus package of needed authorities and passed the original Patriot Act 45 days after the attacks. While not perfect, the Patriot Act was a strong and a necessary piece of legislation. From my first days at the FBI in 2002, I could see the impact these authorities were having on our counterterrorism operations -- from the newly-permitted coordination between law enforcement and intelligence personnel to the enhanced access to business records that are vitally important to a fast-moving

threat investigation. The Patriot Act authorities were having the intended effect -- they were strengthening our capacity to prevent the next 9/11 attack.

With the approach of the 2005 sunsets that were built into the original Patriot Act, Congress undertook to re-examine these authorities and engage in a vigorous debate over their reauthorization. To its enduring credit, Congress went through a lengthy process of carefully scrutinizing each provision and identifying those where additional limitations or oversight could provide protection against misuse without reducing their operational effectiveness. This process resulted in the 2006 Reauthorization Act that provided significant new safeguards for many of the primary authorities in the original Patriot Act. It also made permanent all but two of the sixteen provisions that were scheduled to sunset that year.

With the benefit of that thorough re-examination and eight years of experience with the Patriot Act authorities, we are now at the point of institutionalizing them into the fabric of our counterterrorism operations. Our law enforcement and intelligence communities have adopted the procedures, training and policies to incorporate the new authorities into their operations; they have implemented the additional safeguards imposed by the Reauthorization Act; and they operate subject to substantial oversight by the Foreign Intelligence Surveillance Court (the FISA Court) and by Congress, which receives regular classified reports and briefings on the use of these authorities. And importantly, they are using the Patriot Act tools to significant effect. As FBI Director Mueller has testified, "the PATRIOT Act has changed the way the FBI operates, and . . . many of our operational counterterrorism successes since September 11 are the direct result of the changes incorporated in the PATRIOT Act." Hearing before the Select Committee on Intelligence, April 27, 2005.

III. The Counterterrorism Authorities Subject to Expiration this Year

With the continuing threat from what the President has aptly described as al Qaeda's "far-reaching network of violence and hatred," it is important that our counterterrorism professionals retain the ability to use all of our Patriot Act authorities. This is particularly true of the three provisions that are subject to reauthorization this year. These provisions were born of the harsh lesson of 9/11; they were carefully reviewed by Congress during the reauthorization process and two were augmented with substantial safeguards; and they have been effectively incorporated into our counterterrorism operations with due regard for privacy and civil liberties and with extensive oversight by the FISA Court and Congress. Given this track record, it is now time to institutionalize these authorities, with the clear understanding that Congress can -- and should -- keep a close eye on their use and propose future amendments if it perceives they are being misapplied.

A. Section 206 -- Roving Surveillance Authority

Section 206 of the Patriot Act authorized the government to conduct "roving" surveillance of a foreign power or agent thereof. Previously, national security investigators who were conducting electronic surveillance of a foreign terrorist or spy were required to go back to the FISA Court for a new order every time that target used a different telephone or other communication device. With this new authority, they could now secure authorization to

maintain continuous surveillance as a target moves from one communication device to another -- which is standard tradecraft for many surveillance-conscious terrorists and spies.

This is a critical investigative tool, especially given the proliferation of inexpensive cell phones, calling cards and other innovations that make it easy to dodge surveillance by rotating communication devices. While law enforcement personnel investigating regular crimes like drug trafficking 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 in 2001. Since then, the FBI has used it on approximately 140 occasions, and its use has been "tremendously important" and "essential, given the technology and growth of technology that we've had." Testimony of FBI Director Mueller, Hearing before the Senate Judiciary Committee, September 16, 2009.

While some have raised privacy concerns about this authority, a fair review of Section 206 shows that Congress incorporated a number of safeguards to ensure its judicious and responsible use. First, this new provision did nothing to affect the government's touchstone evidentiary burden; the government must still demonstrate probable cause that the target is a foreign power or an agent of a foreign power. Second, the statute ensures that the FISA Court will closely monitor any roving surveillance; within ten days of conducting roving surveillance on a new communication device, the government is required to give the FISA Court a full report explaining why it believes the target is now using that device and how it will adapt the standard minimization procedures to limit the acquisition, retention and dissemination of communications involving United States persons that might be collected from that surveillance. Finally, the government can use this authority only under limited circumstances; a Section 206 order can issue only if the government provides the FISA Court with "specific facts" demonstrating that actions of the target -- such as switching cell phones -- "may have the effect of thwarting" its ability to identify and conduct surveillance on the communication facility he is using.

These safeguards and the operational need to surveil terrorists and spies as they rotate their phones and other communication devices make a very strong case for reauthorizing the "roving wiretap" authority in Section 206.

B. Section 215 -- Business Records Orders under FISA

Section 215 authorized the FISA Court to issue orders for the production of the same kind of records and other tangible things that law enforcement officers and prosecutors have historically been authorized to acquire through grand jury subpoenas. As a long-time criminal prosecutor, I can tell you that the authority to compel production of business records is absolutely essential to our law enforcement investigations.

Prior to the enactment of Section 215, our national security personnel did not have that authority and they were hamstrung in their effort to obtain business records during international terrorism and espionage investigations. Whereas criminal prosecutors and investigators could issue a subpoena for any record that is relevant to their grand jury investigation, national security personnel could secure a court order only for records that pertain to a person who can be shown by "specific and articulable facts" to be a foreign power or an agent of a foreign power. In

addition, they were permitted to request FISA production orders only for those records held by a business that qualified as "a common carrier, public accommodation facility, physical storage facility or vehicle rental facility." The latter limitation meant, for example, that an agent investigating whether a terrorist had purchased bulk quantities of fertilizer to produce a bomb could not have used a FISA order to obtain the relevant records because a feed store is not "a common carrier, public accommodation facility, physical storage facility or vehicle rental facility."

Section 215 addressed these weaknesses by adopting the relevance standard for issuance of an order and by expanding the reach of this authority to any type of entity. With this new latitude, the Section 215 authority has been used by the FBI on approximately 250 occasions, *id.*, and has "been exceptionally useful" in its national security investigations. Testimony of FBI Director Mueller, Hearing before the House Judiciary Committee, May 20, 2009.

Like the roving surveillance authority, Congress built into Section 215 a panoply of safeguards to protect against misuse. In fact, it is clear that FISA Court orders under Section 215 are significantly more protective of civil liberties than the grand jury subpoenas that are regularly issued by criminal prosecutors around the country. While both authorities require that the records sought are relevant to an authorized investigation, only the Section 215 order requires court approval; a prosecutor, by contrast, can issue a subpoena without any court review at all. Moreover, unlike the grand jury subpoena authority, Section 215 explicitly disallows the issuance of court orders if the underlying investigation is only looking into conduct -- such as political speech or religious worship -- that is protected by the First Amendment. Finally, Section 215 provides for substantial congressional oversight by requiring the Department of Justice to submit detailed reports to Congress about its use of that authority.

In the Reauthorization Act of 2006, Congress added significant new safeguards to this authority. Addressing concerns raised about particularly sensitive records, it imposed the requirement of high-level approval within the FBI before a 215 order could be sought for "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person." It also provided procedures by which the recipient of a 215 order can appeal to the FISA Court to challenge and litigate the validity of the order and the basis for its nondisclosure requirement -- or "gag order."

With these safeguards in place, there is no reason to return to the days when it was easier for prosecutors to secure records in a simple assault prosecution than for national security investigators to obtain records that may help prevent the next 9/11. Section 215 should be reauthorized.

C. The Lone Wolf Provision

Section 6001 of the Intelligence Reform and Terrorism Protection Act (IRTPA) allows the government to conduct surveillance on a non-US person who "engages in international terrorism or activities in preparation therefor" without demonstrating his affiliation to a particular international terrorist organization. When FISA was originally passed in 1978, the contemplated

terrorist target of FISA surveillance was the agent of an organized terrorist group like the Red Brigades or one of the Palestinian terrorist organizations of that era. Today, we face a terrorist adversary in al Qaeda that is a global network of like-minded terrorists -- a network whose membership fluctuates with the shifting of alliances between regional groups. We also face the specter of self-radicalizing foreign terrorists who may not be part of a particular terrorist group, but who are nonetheless just as dangerous and just as committed to pursuing the violent objectives of international terrorism. Given the increasing fluidity in the organization and membership of our international terrorist adversaries, there is a greater likelihood today that we will encounter a foreign terrorist whose affiliation to an identifiable terrorist organization cannot be ascertained. To ensure that the government can surveil such a person, Congress passed the "lone wolf" provision permitting his surveillance based simply on the showing that he is involved in international terrorism. Importantly, this authority can only be used when the target of the surveillance is a non-US person.

The government recently reported that it has not yet used the "lone wolf" provision. Nonetheless, given the threat posed by foreign terrorists -- regardless of affiliation -- and the need to keep them under surveillance, it is important that we keep this authority available for the day when the government may need to use it.

IV. Conclusion

Thank you once again for the opportunity to discuss the sunsetting Patriot Act provisions, their importance to our counterterrorism program, and my reasons for believing they should all be reauthorized this year. I look forward to answering any questions you might have.