AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

WARRANTLESS SURVEILLANCE AND THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: THE ROLE OF CHECKS AND BALANCES IN PROTECTING AMERICANS' PRIVACY RIGHTS (PART II)

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

SEPTEMBER 18, 2007

Serial No. 110–79

Printed for the use of the Committee on the Judiciary

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

U.S. GOVERNMENT PRINTING OFFICE

37–844 PDF WASHINGTON : 2007

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

JOHN CONYERS, JR., Michigan, *Chairman*

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
LINDA T. SANCHEZ, California
STEVE COHEN, Tennessee
HANK JOHNSON, Georgia
BETTY SUTTON, Ohio
LUIS V. GUTIERREZ, Illinois
BRAD SHERMAN, California
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
ARTUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota

LAMAR SMITH, Texas
F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
CHRIS CANNON, Utah
RIC KELLER, Florida
DARRELL ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio

PERRY APELBAUM, *Staff Director and Chief Counsel*
JOSEPH GIBSON, *Minority Chief Counsel*

CONTENTS

SEPTEMBER 18, 2007

Page

OPENING STATEMENTS

The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Chairman, Committee on the Judiciary 1
The Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Ranking Member, Committee on the Judiciary 2
The Honorable Jerrold Nadler, a Representative in Congress from the State of New York, and Member, Committee on the Judiciary 4
The Honorable Trent Franks, a Representative in Congress from the State of Arizona, and Member, Committee on the Judiciary 5
The Honorable Robert C. "Bobby" Scott, a Representative in Congress from the State of Virginia, and Member, Committee on the Judiciary 6
The Honorable J. Randy Forbes, a Representative in Congress from the State of Virginia, and Member, Committee on the Judiciary 7

WITNESSES

The Honorable J. Mike McConnell, Director of National Intelligence
Oral Testimony 9
Prepared Statement 13
The Honorable Kenneth L. Wainstein, Assistant Attorney General for National Security, United States Department of Justice
Oral Testimony 31
Prepared Statement 34

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Article from *The Wall Street Journal*,, dated September 18, 2007, submitted by the Honorable Lamar Smith 101
Article from *Newsweek* magazine, dated May 22, 2006, submitted by the Honorable Steve Cohen 111

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Ranking Member, Committee on the Judiciary 123
Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary 125
Prepared Statement of the Honorable Steve Cohen, a Representative in Congress from the State of Tennessee, and Member, Committee on the Judiciary 133
Questions submitted for the Record to the Honorable J. Mike McConnell, Director of National Intelligence 134
Questions submitted for the Record to the Honorable Kenneth Wainstein, Assistant Attorney General for National Security, United States Department of Justice 155

WARRANTLESS SURVEILLANCE AND THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: THE ROLE OF CHECKS AND BALANCES IN PROTECTING AMERICANS' PRIVACY RIGHTS (PART II)

TUESDAY, SEPTEMBER 18, 2007

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 11:53 a.m., in Room 2141, Rayburn House Office Building, the Honorable John Conyers, Jr. (Chairman of the Committee) presiding.

Present: Representatives Conyers, Berman, Nadler, Scott, Watt, Lofgren, Jackson Lee, Waters, Delahunt, Sánchez, Cohen, Johnson, Sutton, Baldwin, Schiff, Wasserman Schultz, Ellison, Smith, Coble, Lungren, Issa, Pence, Forbes, King, Feeney, Franks, Gohmert, and Jordan.

Staff present: Lou Debaca, Majority Counsel; Perry Apelbaum, Majority Staff Director and Chief Counsel; Michael Volkov, Minority Counsel; and Joseph Gibson, Minority Chief Counsel.

Mr. CONYERS. The Committee will come to order.

Welcome, everyone. Without objection, the Chair is authorized to declare a recess of the Committee, if necessary.

We are here today for the hearing on Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights.

There are few rights that are more fundamental to our democracy than the right to privacy. And there are few powers that are more intrusive or more dangerous than the Government's ability to conduct surveillance on its citizens.

The conflict between this right and these powers go to the very core of who we are as a Nation. For more than 30 years, we have relied on the Foreign Intelligence Surveillance Act to strike the appropriate balance between the Government's need to protect our citizens from foreign attack and our citizens' right to be free from unreasonable searches and seizures.

The heart of that bargain was that Government could indeed use its awesome power to conduct surveillance, but subject to independent court review, although a somewhat cursory and secret court review.

Six years ago, the Administration unilaterally chose to engage in warrantless surveillance of American citizens without court review.

And 6 weeks ago, when the scheme appeared to be breaking down, the Administration insisted that we immediately pass a law they had drafted for us that essentially transferred the power of independent review from the courts to the attorney general. And that was done without hearings.

We are here today to consider whether that was the appropriate course of action and what this Congress can do to restore the proper balance. What we have learned over the last 6 weeks does not give this Chairman much cause for comfort.

First, we have learned that the Administration wrote their bill so broadly and loosely that it permits the Government to intercept any and all electronic communications from United States citizens to anyone even thought to be abroad at the time.

This would include reporters, elected officials and political enemies of the Administration, for example.

Second, we have learned that, also because of the broad manner in which the Administration drafted its bill, the new Government power is not even limited to electronic surveillance.

It could apply to business records, library files, personal mail and even domestic searches of our homes, as long as the foreign person was somehow implicated.

Third, we have learned that even after weeks of negotiations and months of promises, we still have no meaningful oversight either of the old warrantless surveillance program or the new legislation signed in August.

The Senate's subpoenas continue to be ignored, and the House may be on a similar collision course.

The right to privacy is too important to be sacrificed in a last-minute rush before a congressional recess, which is what happened.

The need for national consensus in our efforts to track down terrorists and foil their plots is too important to ignore the constructive concerns of the Congress and the courts.

We on this Committee are ready and willing to work with the Administration, but they need to show us that they are ready to fix this broken law and ready to truly join forces in common cause against terror.

Our system of democracy demands no less, and I am confident that the Committee on the Judiciary in the House of Representatives can accomplish these complex aims.

And I am pleased now to recognize the distinguished Ranking Member of the Judiciary Committee, Lamar Smith, of Texas.

Mr. SMITH. Thank you, Mr. Chairman.

The modernization of the Foreign Intelligence Surveillance Act is one of the most critical issues facing the House Judiciary Committee.

I am encouraged that we have the Director of National Intelligence, Michael McConnell, and the Assistant Attorney General for the National Security Division, Ken Wainstein, here today to provide the Committee with important information on the real-world implications of FISA reform.

This is the first appearance of the Director of National Intelligence before the Judiciary Committee. Director McConnell's intelligence and national security career spans over 30 years. He has served under both Democratic and Republican Presidents, includ-

ing as the director of the National Security Agency in the Clinton administration.

Despite his impressive nonpartisan service in the intelligence community, his motives have been impugned simply because he supports a policy he believes in. Such partisan criticism distracts us from what should be a nonpartisan issue, protecting our country from terrorist attacks.

Foreign terrorists are committed to the destruction of our country. We are at war with sophisticated foreign terrorists who are continuing to plot deadly attacks. It is essential that our intelligence community has the necessary tools to detect and disrupt such attacks.

Foreign terrorists have adapted to our efforts to dismantle their operations. As their terrorist operations evolve, we need to acquire new tools and strategies to respond to their threats.

We have a duty to ensure that the intelligence community can gather all the information they need to protect our country.

In the 30 years since Congress enacted the Foreign Intelligence Surveillance Act, telecommunications technology has dramatically changed and terrorists have employed new techniques to manage and expand their terrorist networks.

Before we left for the August recess, Congress passed important legislation to fill a gap in FISA. We need to make that fix permanent and pass other measures needed to prevent another terrorist attack against our Nation.

FISA does not require a court order to gather foreign communications between foreign terrorists outside the United States. The real issue is this. Should FISA require a court order when a known foreign terrorist communicates with a person inside the United States?

The intelligence community and 30 years of experience under FISA say no. For the last 30 years, FISA never required such an order. Requiring a court order for every phone call from a foreign target to a person inside the U.S. is contrary to FISA and common sense.

How can the intelligence community anticipate a communication from a foreign terrorist to a terrorist inside our country?

In much the same way as a criminal wiretap, FISA provides and has provided for 30 years specific minimization procedures to protect the privacy of persons inside the United States with whom a foreign target may communicate.

It is unclear why now, after all this time, some seek to dismantle rather than modernize FISA. Requiring separate FISA authority for these calls could be a deadly mistake.

Calls between a foreign terrorist and a person located inside the United States should be minimized in accordance with well-established procedures. To do otherwise is to jeopardize the safety of our Nation.

The Director of National Intelligence made it clear that FISA modernization is essential to the intelligence community to protect America from terrorist attacks.

The American people understand what is at stake. Almost 60 percent of Americans polled on the subject of FISA reform supported the Protect America Act. Less than 26 percent opposed it.

The simple fact is that Americans support surveillance of foreign terrorists when they contact persons in the United States.

I look forward to today's hearing with the hope that the debate on FISA reform will lead to enactment of all the director's proposals submitted in April.

These proposals would ensure assistance from private entities in conducting authorized surveillance activities, make certain that private entities are protected from liability for assisting the Government, and streamline the FISA process so that the intelligence community can direct resources to essential operations.

These reforms are long overdue. They should be debated without exaggerated claims of abuse or unfounded horror stories of threats to civil liberties.

We should maintain our commitment to winning the war against terrorism. We must do all that we can to ensure that the words "never again" do, in fact, ring true across our country.

Mr. Chairman, thank you for yielding the time, and I will yield back.

Mr. CONYERS. Thank you, Mr. Smith.

The Chair will now recognize the following Subcommittee Chairmen and Ranking Members for 2.5 minutes each. I will recognize the Ranking Member of the Crime Subcommittee, Randy Forbes; the Chairman of the Subcommittee on Crime, Bobby Scott; the Ranking minority Member on the Constitution Subcommittee, Trent Franks, of Arizona, and we will begin with the Chairman of the Constitution Subcommittee, Jerry Nadler, of New York.

Mr. NADLER. Thank you.

I would like to begin by thanking Chairman Conyers for holding this hearing today.

It is vitally important that we continue to examine the recently enacted White House bill that drastically alters the Foreign Intelligence Surveillance act.

The so-called Protect America Act was rushed through Congress just before the August recess and gives unnecessary license for the Administration to wiretap Americans without court supervision and, in my opinion, to trash the fourth amendment.

I am particularly troubled by the Administration's ongoing charm offensive. We have seen similar campaigns waged around other controversial and over broad programs—the PATRIOT Act, the national security letter authority, the Military Commissions Act and others.

Just last week, the Director of National Intelligence, Michael McConnell, had to retract earlier statements that the act helped German authorities thwart a suspected terrorist plot earlier this month.

Also, Assistant Attorney General Kenneth Wainstein wrote lawmakers to say the act does not authorize physical searches of homes, domestic mail or people's personal effects and computers.

Let's have some truth in advertising. The act gives the President almost unfettered power to spy without traditional approval, not only on foreigners, but on Americans.

The National Security Agency is now permitted without a warrant to access virtually all international communications of Americans with anyone outside the U.S. so long as the Government

maintains that the surveillance is directed at people, including citizens, who are reasonably believed to be located outside the United States, not reasonably believed to be terrorists or in communication with any foreign power, but simply to be outside the United States.

I, for one, have little confidence in what this Administration may consider reasonable in any event. We must not forget the lessons of history. Both the fourth amendment and the Foreign Intelligence Surveillance Act were responses to abuses by Government officials who thought they were above the law.

We all agree that we want to protect our national security and that foreign intelligence gathering is fundamentally different from domestic surveillance. We should, however, also agree that the power to invade people's privacy must not be exercised unchecked.

As we consider how to fix the Protect America Act, we must restore the fundamental freedoms that have been lost because of our recklessness. We must focus surveillance on terrorist activity and provide meaningful court review to protect the rights of Americans who will be spied on in our country.

We must not trust this or any other Administration to police itself. We must act now to restore much-needed checks and balances into this damaged law. We must restore respect for our Constitution that this Administration obviously does not care about.

Thank you. I yield back the balance of my time.

[Applause.]

Mr. CONYERS. Now, everybody in this hearing room knows the rules, so I don't intend to repeat them over and over again.

The Chair now recognizes the gentleman from Arizona, Ranking minority Member of the Constitution Subcommittee, Mr. Trent Franks.

Mr. FRANKS. Well, thank you, Mr. Chairman.

Mr. Chairman, I first want to welcome the Director of National Intelligence, Michael McConnell, and the Assistant Attorney General for the National Security Division, Ken Wainstein, to today's hearing.

I look forward to your efforts and hearing about them, gentlemen, on keeping our country safe and to prevent another terrorist attack on America.

I am hopeful that this hearing will lead to a real-world discussion of the tools needed to protect our country from further attacks.

It has just been over 6 years now since the tragic September 11 attacks against our Nation. And just weeks ago, terrorist plots were disrupted in Germany and Denmark. We are fighting this war on a global front, and American interests are threatened everywhere.

We need to make sure that our intelligence community and law enforcement agencies have all of the tools needed to prevent another attack on our Nation.

The majority has ignored the need for modernizing the Foreign Intelligence Surveillance Act and has adopted rhetoric that boils down to political cover at the expense of national security.

The majority pays homage to the so-called civil liberties groups by ignoring 30 years of practical experience under FISA. They conjure up hypothetical scenarios that are irrelevant or just plain ridiculous to support their claims.

We need to focus this hearing on two primary issues. First, FISA does not apply to foreign communications outside the United States. And second, FISA does not require a court order for calls from a foreign terrorist to a person inside the United States.

The majority agrees with the first point, but simply ignores the second one. My question to the majority is simply this: Please explain how, in practical terms, the intelligence community should monitor foreign terrorists overseas when you argue that calls to the United States require a court order.

Second, what impact will this have on the ability of intelligence communities in our Nation to support and protect our country?

Mr. Chairman, if terrorists are talking outside this country or if terrorists are calling into this country, we better know what they are saying, because their capability to hurt this country will only grow as time passes.

We have a responsibility in Congress to prevent attacks against our country and to protect our communities and our families. Civil liberties are the foundation of our freedom, but such freedom will never exist if we ignore our security.

I am confident that our witnesses will put to rest the inaccuracies and confusions that have surrounded this important issue.

And I yield back. Thank you, Mr. Chairman.

Mr. CONYERS. Thank you.

I thank the gentleman from Arizona.

The Chair recognizes the Chair of the Crime Subcommittee, Mr. Bobby Scott, of Virginia.

Mr. SCOTT. Thank you, Mr. Chairman, and I appreciate your holding these hearings on warrantless surveillance under the Foreign Intelligence Surveillance Act.

Because of the department's refusal to respond to questions for information, we have been stymied in conducting meaningful oversight in this area. At the same time, we find out crucial details about the program through media reports.

So there is a sense that there is now no transparency and virtually no checks and balances on the Administration's discretion on who or what is the subject of warrantless surveillance.

There has never been any controversy over overseas surveillance. You do not need any oversight for that, no warrant, and if technical amendments are needed to clarify that, then those amendments would not be controversial.

But now based on the Administration's own certification, it is free to intercept communications believed to be from outside of the United States into the United States and possibly, even because of, ambiguities in the law, even domestic calls if they concern someone outside of the United States and they involve any vague notion of foreign intelligence.

At a hearing earlier this month we discovered the expansive nature of the bill. Any communications that are concerning the foreign target could be fair game.

And the term "foreign intelligence" does not mean terrorism. It could mean almost anything of interest to foreign affairs, including trade deals, for example.

Finally, the standard the Government has to meet to engage in such data mining is the acquisition of information has to be a sig-

nificant justification for the invasive surveillance techniques, not the traditional primary justification.

So if the Department of Justice wiretaps on foreign intelligence is just a significant purpose and not the primary purpose, you have to wonder what the primary purpose could be, particularly in light of the fact that the Administration has not credibly responded to allegations of partisan politics involved in criminal prosecutions.

I want to emphasize that this is not a question of balancing rights and liberties versus security. The Department of Justice has wide latitude to conduct surveillance under FISA before this statute was amended by the Protect America Act. Virtually all of the department's FISA applications have been approved.

There is even an emergency exception to provide for warrants after the fact. Requirement of a FISA warrant does not prevent a wiretap.

There is nothing you can do under the new protect act that you couldn't already do. You just needed a FISA oversight beforehand. And if you are in a hurry, you can get it after the fact.

Now, without adequate court review, the Department of Justice no longer has to explain or justify how it treats some calls or e-mails of a person in the U.S. when they are intercepted.

This debate is more about complying with the law than it is about maintaining security. Restoring meaningful court oversight will give the public confidence that the Department of Justice is complying with the law.

Thank you, Mr. Chairman.

Mr. CONYERS. Thank you, sir.

The Chair recognizes the Ranking Member of the Crime Subcommittee, the distinguished gentleman from Virginia, Randy Forbes.

Mr. FORBES. Thank you, Mr. Chairman.

I believe this is an important hearing for our witnesses to inform us about gathering foreign intelligence through domestic surveillance as well as the law Congress recently enacted to fix the Foreign Intelligence Surveillance Act.

I wanted to welcome our witnesses and thank them for being here today to answer our questions.

I am sorry for the environment in which you must do that. You deserve better. This Committee deserves better. Our country deserves better.

But I want to thank you for the dedication you have shown to keep us safe despite the personal attacks you must often endure.

Director McConnell has made it clear the Foreign Intelligence Surveillance Act of 1978 needs to be updated. It is imperative that the intelligence community have the ability to effectively monitor foreign terrorists to prevent any future attacks on our country.

Director McConnell has explained to Congress for more than a year that the Government devotes substantial resources to obtaining court approvals to conduct surveillance against terrorists located overseas, a requirement not envisioned by Congress when it enacted FISA.

Foreign intelligence gathering does not occur in a vacuum, and foreign terrorists do not limit their communications to only other terrorists overseas.

Therefore, from its inception, FISA has addressed those instances in which a foreign target communicates with an individual inside the United States.

This law was enacted by a Democratic controlled Congress under a Democratic President but for some reason the majority suddenly has a problem with this provision of FISA.

There is no more simple way to state it: To require a court order for every instance in which a foreign target communicates with someone inside the United States is to require a court order for every foreign target, and requiring this would reverse 30 years of established intelligence gathering and would give the terrorists the upper hand in planning their next attack on America.

The intelligence community cannot possibly know ahead of time who these terrorists will talk to. It needs to have the flexibility to monitor calls that may occur between a foreign terrorist and a person inside the United States.

Such monitoring of these communications can be conducted with well-established minimization rules that have been applied to protect the privacy and civil liberties of U.S. persons.

The Protect America Act and other changes to FISA proposed by Director McConnell are intended to bring foreign intelligence surveillance into the 21st century.

I fear that my colleagues on the other side, if they continue to inflame the debate with unrealistic hypotheticals and partisan posturing, will stymie our Nation's ability to protect itself.

I look forward to hearing from our witnesses, and I yield back the balance of my time.

Mr. CONYERS. Thank you.

Other Members' statements will be included in the record at this point, without objection.

We welcome the two distinguished witnesses here today.

Director of National Intelligence Mike McConnell. Director McConnell has served 29 years in the United States Navy as an intelligence officer, as director of National Security Agency and, after retiring from the Navy at the rank of vice admiral, was senior vice president in the consulting firm of Booz Allen Hamilton, focusing on intelligence and national security concerns, before returning to public service in his current position.

Our second witness of the day is Kenneth Wainstein, Assistant Attorney General for National Security. Mr. Wainstein's service at the department includes service as a career prosecutor in two United States attorneys' offices and as general counsel to the Federal Bureau of Investigation and chief of staff to FBI Director Mueller.

Immediately prior to his current post, Mr. Wainstein was U.S. attorney for the District of Columbia.

Your written statements will be made part of the record in their entirety. You know the rules of engagement here. And given the gravity of the issues under discussion and the key roles you play, we would appreciate it if you would take an oath before you begin your testimony.

Please stand and raise your right hand. Do you solemnly swear or affirm under penalty of perjury that the testimony you are about

to provide the Committee will be the truth, the whole truth and nothing but the truth, so help you God?

All the witnesses indicated in the affirmative.

Please be seated.

Greetings, Admiral McConnell. You may begin the hearing with your statement.

TESTIMONY OF J. MIKE McCONNELL, DIRECTOR OF NATIONAL INTELLIGENCE

Mr. MCCONNELL. Good afternoon, Mr. Chairman, Members of the Committee. Thank you for inviting me to appear today in my capacity as the head of the United States intelligence community.

I appreciate this opportunity to discuss the act in question, the Protect America Act, and the need for lasting modernization of the Foreign Intelligence Surveillance Act, as we will refer to in the hearing as FISA.

I am pleased to be joined today by my General Counsel, Ben Powell, sitting to my right, and Assistant Attorney General, as has been noted, Ken Wainstein, of the Department of Justice National Security Division.

Before I begin, I need to note that some of the specifics that support my testimony cannot be discussed in open session.

I understand and am sensitive to the fact that FISA and the Protect America Act and the types of activities that these laws govern are of significant interest to the Congress and to the public.

And for that reason, I will be as open as I can, but such discussions do come with a degree of risk. This is because open discussion of specific foreign intelligence collection capabilities could cause us to lose those very same capabilities.

Therefore, on certain specific issues, I will be happy to discuss further with Members in a classified setting, which I understand we might have later today.

When I was preparing for my confirmation hearing, as you can imagine, I did lots of reading. I went back to read the 9/11 Commission. I read the WMD Commission. And I read the joint congressional inquiry into 9/11.

And I want to quote from the joint congressional inquiry. "The joint inquiry has learned that many of the future hijackers communicated with a known terrorist facility in the Middle East while he was living in the United States.

"The intelligence community did not identify the domestic origin of those communications prior to September 11 so that additional FBI investigative efforts could be coordinated."

Despite this country's substantial advantages, there was insufficient focus on what many would have thought was among the most critically important kinds of terrorist-related communications, at least in terms of protecting the homeland.

It is my belief that the first responsibility of the intelligence community is to achieve understanding and secondly to provide warning from that understanding.

As the head of the Nation's intelligence community, it is not only my desire but my duty to encourage changes in policies and procedures and, where needed, legislation to improve our ability to provide warning of terrorist or other threats to our country.

On taking this post, it became clear to me that our intelligence capability was being degraded. I learned that collection using authorities provided by FISA continued to be instrumental in protecting the Nation, but due to changes in technology the law was actually preventing us from collecting needed intelligence.

I asked what we could do to correct the problem. I learned that the Congress and a number of intelligence professionals had been working on this issue already.

In fact, in July 2006, over a year ago, the Director of NSA, General Keith Alexander, and the Director of CIA, General Mike Hayden, testified before the Senate Judiciary Committee regarding proposals to update FISA.

I also learned that Members of Congress on both sides of the aisle had proposed legislation to modernize FISA. A bill passed this body, the House, last year. A similar bill did not pass—although introduced, did not pass on the Senate side.

And so dialogue on FISA has been ongoing for some time. This has been constructive dialogue, and I hope it continues in furtherance of serving the Nation's interest to protect our citizens.

None of us want a repeat of the 9/11 attacks, although al-Qaida has stated their intention to conduct another such attack.

FISA is the Nation's statute for conducting electronic surveillance and physical search for foreign intelligence purposes. I emphasize foreign intelligence purposes.

When passed in 1978, FISA was carefully crafted to balance the Nation's need to collect foreign intelligence information with a need for protection of civil liberties and privacy rights of our citizens.

The 1978 law created a special court, the Foreign Intelligence Surveillance Court. The court's members devote a considerable amount of their time and effort, while at the same time fulfilling their district court responsibilities. We are indeed grateful for their service.

FISA is a very, very complex statute. It has a number of substantial requirements. Detailed applications contain extensive factual information and require approval by several high-ranking members of the executive branch before they can even go to the court.

The applications are carefully prepared, subject to multiple layers of review for legal as well as factual sufficiency. It is my steadfast belief that the balance that the Congress struck in 1978 was not only elegant, it was the right balance.

Why do we need the changes that the Congress passed just last August? FISA's definition of electronic surveillance simply did not keep pace with technology. Let me explain what I mean by that.

FISA was enacted before cell phones, before e-mail and before the Internet was a tool used by hundreds of millions of people around the world every day, to include terrorists.

When the law was passed in 1978, almost all local calls were on a wire and almost all international communications were in the air, or how we would refer to it as wireless communications.

Therefore, FISA was written in 1978 to distinguish between collection on a wire and collection out of the air. Today, the situation from 1978 is completely reversed. Most international communications are on a wire, fiber optic cable, and local calls most often are in the air.

FISA also originally placed a premium on the location of the collection. Because of these changes in technology, communications intended to be excluded from FISA in 1978 were frequently included in the current interpretation. This had real consequences.

It meant that the intelligence community in a significant number of cases was required to demonstrate probable cause to a court in order to target for surveillance a communication of a foreign person located overseas.

Because of this, the old FISA requirements prevented the intelligence community from collecting important foreign intelligence information on current terrorist threats.

In the debate over the summer and since, I have heard individuals from both inside and outside the Government assert that threats to our Nation do not justify this authority. Indeed, I have been accused of exaggerating the threats that face our Nation.

Allow me to attempt to dispel this notion. The threats that we face are real and they are, indeed, serious. In July of this year, we released a National Intelligence Estimate, commonly referred to as an NIE, on the terrorist threat to the homeland.

An NIE is coordinated among all 16 agencies of the community, and it is the intelligence community's most authoritative written judgment on a particular subject.

The key judgments from this NIE are posted on our Web site, DNI.gov. I would encourage Members and our citizens to read the posted NIE judgments.

In short, these assessments conclude the following. The United States will face a persistent and evolving terrorist threat over the next 3 years. That is the period of the NIE.

The main threat comes from Islamic terrorist groups and cells and especially al-Qaida. Al-Qaida continues to coordinate with regional terrorist groups such as al-Qaida in Iraq, across North Africa and in other regions.

Al-Qaida is likely to continue to focus on prominent political, economic and infrastructure targets, with a goal of producing mass casualties—with a goal of producing mass casualties—visually dramatic destruction, significant economic aftershock and fear among the United States population.

These terrorists are weapons proficient, they are innovative and they are persistent. Al-Qaida will continue to acquire chemical, biological, radiological and nuclear material for attack, and they will use them given the opportunity.

Globalization trends and technology continue to enable even small groups of alienated people to find and connect with one another, justify and intensify their anger, and mobilize resources for attack, all without requiring a centralized terrorist organization, training camp or a leader.

This is the threat we face today, and one that our intelligence community is challenged to counter. Moreover——

Mr. CONYERS. The gentleman's time is nearly up.

Mr. MCCONNELL. Moreover, the threats we face as a Nation are not limited to terrorism. It also includes weapons of mass destruction.

The Protect America Act updated FISA and passed by the Congress, signed by the President on the 5th of August, has already made the Nation safer.

After the law was enacted, we took immediate action to close critical foreign intelligence gaps related to terrorist threats.

I want to close with noting five pillars in the law that enabled us to do our mission.

It clarified that the definition of electronic surveillance under FISA should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States. That is a very, very important feature.

Under the act, we are now required to submit to the FISA court for approval the procedures that we used to determine that the target of acquisition is located outside the United States. This portion is new and was added to give the Congress and the public more confidence in the process.

In addition to oversight by the Congress, the new FISA process allows review of the procedures by the FISA court.

A third thing was the act allows the attorney general and the DNI to direct third parties to cooperate with us to acquire foreign intelligence information.

Fourth, the act provides limited liability protection for private parties who assist us when complying with lawful directives issued under the FISA Act.

And most importantly, the one which I personally identify, FISA as amended continues to require that we obtain a court order to conduct electronic surveillance or physical search against all persons located inside the United States.

I want to assure the Congress that we will cooperate in executing this law, subject to the appropriate oversight not only by the Congress but by the court.

Sir, that concludes my opening statement.

[The prepared statement of Mr. McConnell follows:]

PREPARED STATEMENT OF THE HONORABLE J. MIKE MCCONNELL

STATEMENT FOR THE RECORD OF
J.M. McCONNELL
DIRECTOR OF NATIONAL INTELLIGENCE

BEFORE THE
JUDICIARY COMMITTEE
HOUSE OF REPRESENTATIVES

September 18, 2007

Good morning Chairman Conyers, Ranking Member Smith, and Members of the Committee.

Thank you for inviting me to appear here today in my capacity as head of the United States Intelligence Community (IC). I appreciate this opportunity to discuss the 2007 Protect America Act; updating the Foreign Intelligence Surveillance Act; and our implementation of this important new authority that allows us to more effectively collect timely foreign intelligence information. I look forward to discussing the need for lasting modernization of the Foreign Intelligence Surveillance Act (FISA), including providing liability protection for the private sector. I am pleased to be joined here today by my General Counsel, Ben Powell, and Assistant Attorney General Ken Wainstein of the Department of Justice's National Security Division.

Before I begin, I need to note that some of the specifics that support my testimony cannot be discussed in open session. I understand, and am sensitive to the fact, that FISA and the Protect America Act and the types of activities these laws govern, are of significant interest to Congress and to the public. For that reason, I will be as open as I can, but such discussion comes with degrees of risk. This is because open discussion of specific foreign intelligence collection capabilities could cause us to lose those very same capabilities. Therefore, on certain specific issues, I am happy to discuss matters further with Members in a classified setting.

I have not appeared before this Committee previously as a witness, and so I would like to take a moment to introduce myself to you. I am a career intelligence professional. I spent the majority of my career as a Naval

Intelligence Officer. During the periods of Desert Shield and Desert Storm, as well as during the dissolution of the Soviet Union, I served as the primary Intelligence Officer for the Chairman of the Joint Chiefs of Staff and the Secretary of Defense. I then had the privilege of serving as the Director of the National Security Agency (NSA) from 1992 to 1996, under President Clinton. In 1996, I retired from the U.S. Navy after 29 years of service - 26 of those years spent as a career Intelligence Officer. I then turned to the private sector as a consultant, where for ten years I worked to help the government achieve better results on a number of matters, including those concerning intelligence and national security. I have been in my current capacity as the nation's second Director of National Intelligence (DNI) since February 2007.

It is my belief that the first responsibility of intelligence is to achieve understanding and to provide warning. As the head of the nation's Intelligence Community, it is not only my desire, but my duty, to encourage changes to policies and procedures, and where needed, legislation, to improve our ability to provide warning of terrorist or other threats to our security. To that end, very quickly upon taking up this post, it became clear to me that our foreign intelligence collection capability was being degraded. This degradation was having an increasingly negative impact on the IC's ability to provide warning to the country. In particular, I learned that our collection using the authorities provided by FISA were instrumental in protecting the nation from foreign security threats, but that, due to changes in technology, the law was actually preventing us from collecting additional foreign intelligence information needed to provide insight, understanding and warning about threats to Americans.

And so I turned to my colleagues in the Intelligence Community to ask what we could do to fix this problem, and I learned that a number of intelligence professionals had been working on this issue for some time already. In fact, over a year ago, in July 2006, the Director of the National Security Agency (NSA), Lieutenant General Keith Alexander, and the Director of the Central Intelligence Agency (CIA), General Mike Hayden, testified before the Senate Judiciary Committee regarding proposals that were being considered to update FISA.

Also, over a year ago, Members of Congress were concerned about FISA, and how its outdated nature had begun to erode our intelligence collection capability. Accordingly, since 2006, Members of Congress on

both sides of the aisle have proposed legislation to modernize FISA. The House passed a bill last year. And so, while the Protect America Act is new, the dialogue among Members of both parties, as well as between the Executive and Legislative branches, has been ongoing for some time. In my experience, this has been a constructive dialogue, and I hope that this exchange continues in furtherance of serving the nation well.

The Balance Achieved By FISA

The Foreign Intelligence Surveillance Act, or FISA, is the nation's statute for conducting electronic surveillance and physical search for foreign intelligence purposes. FISA was passed in 1978, and was carefully crafted to balance the nation's need to collect foreign intelligence information with the protection of civil liberties and privacy rights. I find it helpful to remember that while today's political climate is charged with a significant degree of alarm about activities of the Executive Branch going unchecked, the late 1970's were even more intensely changed by extensively documented Government abuses. We must be ever mindful that FISA was passed in the era of Watergate and in the aftermath of the Church and Pike investigations, and therefore this foundational law has an important legacy of protecting the rights of Americans. Changes we make to this law must honor that legacy to protect Americans, both in their privacy and against foreign threats.

FISA is a complex statute, but in short it does several things. The 1978 law provided for the creation of a special court, the Foreign Intelligence Surveillance Court, which is comprised of federal district court judges who have been selected by the Chief Justice to serve. The Court's members devote a considerable amount of time and effort, over a term of seven years, serving the nation in this capacity, while at the same time fulfilling their district court responsibilities. We are grateful for their service.

The original 1978 FISA provided for Court approval of electronic surveillance operations against foreign powers and agents of foreign powers, within the United States. Congress crafted the law specifically to exclude the Intelligence Community's surveillance operations against targets outside the United States, including where those targets were in communication with Americans, so long as the U.S. side of that communication was not the real target.

FISA has a number of substantial requirements, several of which I will highlight here. A detailed application must be made by an Intelligence Community agency, such as the Federal Bureau of Investigation (FBI), through the Department of Justice, to the FISA Court. The application must be approved by the Attorney General, and certified by another high ranking national security official, such as the FBI Director. The applications that are prepared for presentation to the FISA Court contain extensive information. For example, an application that targets an agent of an international terrorist group might include detailed facts describing the target of the surveillance, the target's activities, the terrorist network in which the target is believed to be acting on behalf of, and investigative results or other intelligence information that would be relevant to the Court's findings. These applications are carefully prepared, subject to multiple layers of review for legal and factual sufficiency, and often resemble finished intelligence products.

Once the Government files its application with the Court, a judge reads the application, conducts a hearing as appropriate, and makes a number of findings, including that there is probable cause that the target of the surveillance is a foreign power or an agent of a foreign power, and that the facilities that will be targeted are used or about to be used by the target. If the judge does not find that the application meets the requirements of the statute, the judge can either request additional information from the government, or deny the application. These extensive findings, including the requirement of probable cause, are intended to apply to persons inside the United States.

It is my steadfast belief that the balance struck by Congress in 1978 was not only elegant, it was the right balance: it safeguarded privacy protection and civil liberties for those inside the United States by requiring Court approval for conducting electronic surveillance within the country, while specifically allowing the Intelligence Community to collect foreign intelligence against foreign intelligence targets located overseas. I believe that balance is the correct one, and I look forward to working with you to maintaining that balance to protect our citizens as we continue our dialogue to achieve lasting FISA modernization.

Technology Changed

Why did we need the changes that the Congress passed in August? FISA's definition of electronic surveillance, prior to the Protect America Act and as passed in 1978, has not kept pace with technology. Let me explain what I mean by that. FISA was enacted before cell phones, before e-mail, and before the Internet was a tool used by hundreds of millions of people worldwide every day. When the law was passed in 1978, almost all local calls were on a wire and almost all international communications were in the air, known as "wireless" communications. Therefore, FISA was written to distinguish between collection on a wire and collection out of the air.

Now, in the age of modern telecommunications, the situation is completely reversed; most international communications are on a wire and local calls are in the air. Communications technology has evolved in ways that have had unfortunate consequences under FISA. Communications that, in 1978, would have been transmitted via radio or satellite, are now transmitted principally via fiber optic cables. While Congress in 1978 specifically excluded from FISA's scope radio and satellite communications, certain "in wire" or fiber optic cable transmissions fell under FISA's definition of electronic surveillance. Congress' intent on this issue is clearly stated in the legislative history:

> "the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States."

Thus, technological changes have brought within FISA's scope communications that the 1978 Congress did not intend to be covered.

Similarly, FISA originally placed a premium on the location of the collection. Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today a single communication can transit the world even if the two people communicating are only a few miles apart.

And yet, simply because our law has not kept pace with our technology, communications intended to be excluded from FISA, were included. This has real consequences to our men and women in the IC working to protect the nation from foreign threats.

For these reasons, prior to Congress passing the Protect America Act last month, in a significant number of cases, IC agencies were required to make a showing of probable cause in order to target for surveillance the communications of a foreign intelligence target located overseas. Then, they needed to explain that probable cause finding in documentation, and obtain approval of the FISA Court to collect against a foreign terrorist located in a foreign country. Frequently, although not always, that person's communications were with another foreign person located overseas. In such cases, prior to the Protect America Act, FISA's requirement to obtain a court order, based on a showing of probable cause, slowed, and in some cases prevented altogether, the Government's ability to collect foreign intelligence information, without serving any substantial privacy or civil liberties interests.

National Security Threats

In the debate surrounding Congress passing the Protect America Act, I heard a number of individuals, some from within the government, some from the outside, assert that there really was no substantial threat to our nation justifying this authority. Indeed, I have been accused of exaggerating the threats that face our nation.

Allow me to dispel that notion.

The threats we face are real, and they are serious.

In July 2007 we released the National Intelligence Estimate (NIE) on the Terrorist Threat to the U.S. Homeland. An NIE is the IC's most authoritative, written judgment on a particular subject. It is coordinated among all 16 Agencies in the IC. The key judgments are posted on our website at dni.gov. I would urge our citizens to read the posted NIE judgments. The declassified judgments of the NIE include the following:

- The U.S. Homeland will face a persistent and evolving terrorist threat over the next three years. The main threat comes from Islamic terrorist groups and cells, especially al-Qa'ida, driven by their undiminished intent to attack the Homeland and a continued effort by these terrorist groups to adapt and improve their capabilities.

- Greatly increased worldwide counterterrorism efforts over the past five years have constrained the ability of al-Qa'ida to attack the U.S. Homeland again and have led terrorist groups to perceive the Homeland as a harder target to strike than on 9/11.

- Al-Qa'ida is and will remain the most serious terrorist threat to the Homeland, as its central leadership continues to plan high-impact plots, while pushing others in extremist Sunni communities to mimic its efforts and to supplement its capabilities. We assess the group has protected or regenerated key elements of its Homeland attack capability, including: a safehaven in the Pakistan Federally Administered Tribal Areas (FATA), operational lieutenants, and its top leadership. Although we have discovered only a handful of individuals in the United States with ties to al-Qa'ida senior leadership since 9/11, we judge that al-Qa'ida will intensify its efforts to put operatives here. As a result, we judge that the United States currently is in a heightened threat environment.

- We assess that al-Qa'ida will continue to enhance its capabilities to attack the Homeland through greater cooperation with regional terrorist groups. Of note, we assess that al-Qa'ida will probably seek to leverage the contacts and capabilities of al-Qa'ida in Iraq.

- We assess that al-Qa'ida's Homeland plotting is likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties, visually dramatic destruction, significant economic aftershocks, and/or fear among the U.S. population. The group is proficient with conventional small arms and improvised explosive devices, and is innovative in creating new capabilities and overcoming security obstacles.

- We assess that al-Qa'ida will continue to try to acquire and employ chemical, biological, radiological, or nuclear material in attacks and would not hesitate to use them if it develops what it deems is sufficient capability.

- We assess Lebanese Hizballah, which has conducted anti-U.S. attacks outside the United States in the past, may be more likely to consider

attacking the Homeland over the next three years if it perceives the United States as posing a direct threat to the group or Iran.

- We assess that globalization trends and recent technological advances will continue to enable even small numbers of alienated people to find and connect with one another, justify and intensify their anger, and mobilize resources to attack—all without requiring a centralized terrorist organization, training camp, or leader.

Moreover, the threats we face as a nation are not limited to terrorism, nor is foreign intelligence information limited to information related to terrorists and their plans. Instead, foreign intelligence information as defined in FISA includes information about clandestine intelligence activities conducted by foreign powers and agents of foreign powers; as well as information related to our conduct of foreign affairs and national defense.

In particular, the Intelligence Community is devoting substantial effort to countering the proliferation of weapons of mass destruction (WMD). State sponsored WMD programs and the risk of WMD being obtained by transnational terrorist networks are extremely dangerous threats we face. China and Russia's foreign intelligence services are among the most aggressive in collecting against sensitive and protected U.S. systems, facilities, and development projects, and their efforts are approaching Cold War levels. Foreign intelligence information concerning the plans, activities and intentions of foreign powers and their agents is critical to protect the nation and preserve our security.

What Does the Protect America Act Do?

The Protect America Act, passed by Congress and signed into law by the President on August 5, 2007, has already made the nation safer by allowing the Intelligence Community to close existing gaps in our foreign intelligence collection. After the Protect America Act was signed we took immediate action to close critical foreign intelligence gaps related to the terrorist threat, particularly the pre-eminent threats to our national security. The Protect America Act enabled us to do this because it contained the following five pillars:

First, it clarified that the definition of electronic surveillance under FISA should not be construed to encompass surveillance directed at a person

reasonably believed to be located outside the United States. This provision is at the heart of this legislation: its effect is that the IC must no longer obtain court approval when the target of the acquisition is a foreign intelligence target located outside the United States.

This change was critical, because prior to the Protect America Act, we were devoting substantial expert resources towards preparing applications that needed FISA Court approval. This was an intolerable situation, as substantive experts, particularly IC subject matter and language experts, were diverted from the job of analyzing collection results and finding new leads, to writing justifications that would demonstrate their targeting selections would satisfy the statute. Moreover, adding more resources would not solve the fundamental problem: this process had little to do with protecting the privacy and civil liberties of Americans. These were foreign intelligence targets, located in foreign countries. And so, with the Protect America Act, we are able to return the balance struck by Congress in 1978.

Second, the Act provides that the FISA Court has a role in determining that the procedures used by the IC to determine that the target is outside the United States are reasonable. Specifically, the Attorney General must submit to the FISA Court the procedures we use to make that determination.

Third, the Act provides a mechanism by which communications providers can be compelled to cooperate. The Act allows the Attorney General and DNI to direct communications providers to provide information, facilities and assistance necessary to acquire information when targeting foreign intelligence targets located outside the United States.

Fourth, the Act provides liability protection for private parties who assist the IC, when complying with a lawful directive issued pursuant to the Protect America Act.

And fifth, and importantly, FISA, as amended by the Protect America Act, continues to require that we obtain a court order to conduct electronic surveillance or physical search when targeting persons located in the United States.

By passing this law, Congress gave the IC the ability to close critical intelligence gaps. When I talk about a gap, what I mean is foreign

intelligence information that we should have been collecting, that we were not collecting. We were not collecting this important foreign intelligence information because, due solely to changes in technology, FISA would have required that we obtain court orders to conduct electronic surveillance of foreign intelligence targets located outside the United States. This is not what Congress originally intended. These items:

- removing targets located outside the United States from the definition of electronic surveillance;
- providing for Court review of the procedures by which we determine that the acquisition concerns persons located outside the United States;
- providing a means to compel the assistance of the private sector;
- liability protection; and
- the continued requirement of a court order to target those within the United States,

are the pillars of the Protect America Act, and I look forward to working with Members of both parties to make these provisions permanent.

Common Misperceptions About the Protect America Act

In the public debate over the course of the last month since Congress passed the Act, I have heard a number of incorrect interpretations of the Protect America Act. The Department of Justice has sent a letter to this Committee explaining these incorrect interpretations.

To clarify, we are not using the Protect America Act to change the manner in which we conduct electronic surveillance or physical search of Americans abroad. The IC has operated for nearly 30 years under section 2.5 of Executive Order 12333, which provides that the Attorney General must make an individualized finding that there is probable cause to believe that an American abroad is an agent of a foreign power, before the IC may conduct electronic surveillance or physical search of that person. These determinations are reviewed for legal sufficiency by the same group of career attorneys within the Department of Justice who prepare FISA applications. We have not, nor do we intend to change our practice in that respect. Executive Order 12333 and this practice has been in place since 1981.

The motivation behind the Protect America Act was to enable the Intelligence Community to collect foreign intelligence information when targeting persons reasonably believed to be outside the United States in order to protect the nation and our citizens from harm. Based on my discussions with many Members of Congress, I believe that there is substantial, bipartisan support for this principle. There are, however, differences of opinion about how best to achieve this goal. Based on the experience of the Intelligence Community agencies that do this work every day, I have found that some of the alternative proposals would not be viable.

For example, some have advocated for a proposal that would exclude only "foreign-to-foreign" communications from FISA's scope. I have, and will continue to, oppose any proposal that takes this approach for the following reason: it will not correct the problem our intelligence operators have faced. Eliminating from FISA's scope communications between foreign persons outside the United States will not meet our needs in two ways:

First, it would not unburden us from obtaining Court approval for communications obtained from foreign intelligence targets abroad. This is because an analyst cannot know, in many cases, prior to requesting legal authority to target a particular foreign intelligence target abroad, with whom that person will communicate. This is not a matter of legality, or even solely of technology, but merely of common sense. If the statute were amended to carve out communications between foreigners from requiring Court approval, the IC would still, in many cases and in an abundance of caution, have to seek a Court order anyway, because an analyst would not be able to demonstrate, with certainty, that the communications that would be collected would be exclusively between persons located outside the United States.

Second, one of the most important and useful pieces of intelligence we could obtain is a communication from a foreign terrorist outside the United States to a previously unknown "sleeper" or coconspirator inside the United States. Therefore, we need to have agility, speed and focus in collecting the communications of foreign intelligence targets outside the United States who may communicate with a "sleeper" or coconspirator who is inside the United States.

Moreover, such a limitation is unnecessary to protect the legitimate privacy rights of persons inside the United States. Under the Protect America Act, we have well established mechanisms for properly handling communications of U.S. persons that may be collected incidentally. These procedures, referred to as minimization procedures, have been used by the IC for decades. Our analytic workforce has been extensively trained on using minimization procedures to adequately protect U.S. person information from being inappropriately disseminated.

The minimization procedures that Intelligence Community agencies follow are Attorney General approved guidelines issued pursuant to Executive Order 12333. These minimization procedures apply to the acquisition, retention and dissemination of U.S. person information. These procedures have proven over time to be both a reliable and practical method of ensuring the constitutional reasonableness of IC's collection activities.

In considering our proposal to permanently remove foreign intelligence targets located outside the United States from FISA's court approval requirements, I understand that there is concern that we would use the authorities granted by the Protect America Act to effectively target a person in the United States, by simply saying that we are targeting a foreigner located outside the United States. This is what has been referred to as "reverse targeting."

Let me be clear on how I view reverse targeting: it is unlawful. Again, we believe the appropriate focus for whether court approval should be required, is <u>who</u> the target is, and <u>where</u> the target is located. If the target of the surveillance is a person inside the United States, then we seek FISA Court approval for that collection. Similarly, if the target of the surveillance is a U.S. person outside the United States, then we obtain Attorney General approval under Executive Order 12333, as has been our practice for decades. If the target is a foreign person located overseas, consistent with FISA today, the IC should not be required to obtain a warrant.

Moreover, for operational reasons, the Intelligence Community has little incentive to engage in reverse targeting. If a foreign intelligence target who poses a threat is located within the United States, then we would want to investigate that person more fully. In this case, reverse targeting would be an ineffective technique for protecting against the activities of a foreign intelligence target located inside the United States. In order to conduct

electronic surveillance or physical search operations against a person in the United States, the FBI, which would conduct the investigation, would seek FISA Court approval for techniques that, in a law enforcement context, would require a warrant.

Oversight of the Protect America Act

Executive Branch Oversight

I want to assure the Congress that we are committed to conducting meaningful oversight of the authorities provided by the Protect America Act. The first tier of oversight takes place within the agency implementing the authority. The implementing agency employs a combination of training, supervisory review, automated controls and audits to monitor its own compliance with the law. Internal agency reviews will be conducted by compliance personnel in conjunction with the agency Office of General Counsel and Office of Inspector General, as appropriate. Intelligence oversight and the responsibility to minimize U.S. person information is deeply engrained in our culture.

The second tier of oversight is provided by outside agencies. Within the Office of the Director of National Intelligence (ODNI), the Office of General Counsel and the Civil Liberties Protection Officer are working closely with the Department of Justice's National Security Division to ensure that the Protect America Act is implemented lawfully, and thoughtfully.

Within fourteen days of the first authorization under the Act, attorneys from my office and the National Security Division conducted their first onsite oversight visit to one IC agency. This first oversight visit included an extensive briefing on how the agency is implementing the procedures used to determine that the target of the acquisition is a person reasonably believed to be located outside the United States. Oversight personnel met with the analysts conducting day-to-day operations, reviewed their decision making process, and viewed electronic databases used for documentation that procedures are being followed. Oversight personnel were also briefed on the additional mandatory training that will support implementation of Protect America Act authorities. The ODNI and National Security Division performed a follow-up visit to the agency shortly thereafter, and will continue periodic oversight reviews.

FISA Court Oversight

The third tier of oversight is the FISA Court. Section 3 of the Protect America Act requires that:

> (a) No later than 120 days after the effective date of this Act, the Attorney General shall submit to the Court established under section 103(a), the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance. The procedures submitted pursuant to this section shall be updated and submitted to the Court on an annual basis.

The Department of Justice has already submitted procedures to the FISA Court pursuant to this section. We intend to file the procedures used in each authorization promptly after each authorization.

Congressional Oversight

The fourth tier of oversight is the Congress. The Intelligence Community is committed to providing Congress with the information it needs to conduct timely and meaningful oversight of our implementation of the Protect America Act. To that end, the Intelligence Community has provided Congressional Notifications to the House and Senate Intelligence Committees regarding authorizations that have been made to date. We will continue that practice. In addition, the Intelligence Committees have been provided with copies of certifications the Attorney General and I executed pursuant to section 105B of FISA, the Protect America Act, along with additional supporting documentation. We also intend to provide appropriately redacted documentation, consistent with the protection of sources and methods, to Members of this Committee and the Senate Judiciary Committee, along with appropriately cleared professional staff.

Since enactment, the Congressional Intelligence Committees have taken an active role in conducting oversight, and the agencies have done our best to accommodate the requests of staff by making our operational and oversight personnel available to brief staff as often as requested.

Within 72 hours of enactment of the Protect America Act, Majority and Minority professional staff of the House Permanent Select Committee on Intelligence requested a briefing on implementation. We made a multi-agency implementation team comprised of eight analysts, oversight personnel and attorneys available to eight Congressional staff members for a site visit on August 9, 2007, less than five days after enactment. In addition, representatives from the ODNI Office of General Counsel and the ODNI Civil Liberties Protection Officer participated in this briefing.

On August 14, 2007, the General Counsel of the FBI briefed House Intelligence Committee staff members regarding the FBI's role in Protect America Act implementation. Representatives from DOJ's National Security Division and ODNI Office of General Counsel supported this briefing.

On August 23, 2007, an IC agency hosted four House Intelligence Committee staff members for a Protect America Act implementation update. An implementation team comprised of thirteen analysts and attorneys were dedicated to providing that brief.

On August 28, 2007, Majority and Minority professional staff from the House Intelligence Committee conducted a second onsite visit at an IC agency. The agency made available an implementation team of over twenty-four analysts, oversight personnel and attorneys. In addition, representatives from ODNI Office of General Counsel, ODNI Civil Liberties and Privacy Office and the National Security Division participated in this briefing.

On September 7, 2007, nineteen professional staff members from the Senate Intelligence Committee and two staff members from the Senate Judiciary Committee conducted an onsite oversight visit to an IC agency. The agency assembled a team of fifteen analysts, oversight personnel and attorneys. In addition, representatives from ODNI Office of General Counsel, ODNI Civil Liberties and Privacy Office and DOJ's National Security Division participated in this briefing.

On September 12, 2007, at the request of the professional staff of the Senate Intelligence Committee, the Assistant Attorney General of the National Security Division, and the General Counsels of the ODNI, NSA, and FBI briefed staff members from the House Intelligence Committee, and the Senate Intelligence, Judiciary and Armed Services Committees regarding

the implementation of the Protect America Act. In all, over twenty Executive Branch officials involved in Protect America Act implementation supported this briefing.

Also on September 12, 2007, an IC agency provided an implementation briefing to two Members of Congress who serve on the House Intelligence Committee and four of that Committee's staff members. Sixteen agency analysts and attorneys participated in this briefing.

On September 13, 2007, four House Intelligence Committee staff members and the Committee's Counsel observed day-to-day operations alongside agency analysts.

On September 14, 2007, an IC agency implementation team of ten analysts briefed three Senate Intelligence Committee and one House Judiciary Committee staff member. The ODNI Civil Liberties Protection Officer and representatives from the Department of Justice supported this visit.

Additional Member and staff briefings are scheduled to take place this week.

Lasting FISA Modernization

I ask your partnership in working for a meaningful update to this important law that assists us in protecting the nation while protecting our values. There are three key areas that I look forward to working with Members of this Committee to update FISA.

Making the Changes Made by the Protect America Act Permanent

For the reasons I have outlined today, it is critical that FISA's definition of electronic surveillance be amended permanently so that it does not cover foreign intelligence targets reasonably believed to be located outside of the United States. The Protect America Act achieved this goal by making clear that FISA's definition of electronic surveillance should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States. This change enabled the Intelligence Community to quickly close growing gaps in our collection related to terrorist threats. Over time, this provision will also enable us to do

a better job of collecting foreign intelligence on a wide range of issues that relate to our national defense and conduct of foreign affairs.

Liability Protection

I call on Congress to act swiftly to provide liability protection to the private sector. Those who assist the government keep the country safe should be protected from liability. This includes those who are alleged to have assisted the government after September 11, 2001. It is important to keep in mind that, in certain situations, the Intelligence Community needs the assistance of the private sector to protect the nation. We cannot "go it alone." It is critical that we provide protection to the private sector so that they can assist the Intelligence Community protect our national security, while adhering to their own corporate fiduciary duties.

I appreciate that Congress was not able to address this issue comprehensively at the time that the Protect America Act was passed, however, providing this protection is critical to our ability to protect the nation and I ask for your assistance in acting on this issue promptly.

Streamlining the FISA Process

In the April 2007 bill that we submitted to Congress, we asked for a number of streamlining provisions to that would make processing FISA applications more effective and efficient. For example, eliminating the inclusion of information that is unnecessary to the Court's determinations should no longer be required to be included in FISA applications. In addition, we propose that Congress increase the number of senior Executive Branch national security officials who can sign FISA certifications; and increase the period of time for which the FISA Court could authorized surveillance concerning non-U.S. person agents of a foreign power, and renewals of surveillance it had already approved.

We also ask Congress to consider extending FISA's emergency authorization time period, during which the government may initiate surveillance or search before obtaining Court approval. We propose that the emergency provision of FISA be extended from 72 hours to one week. This change will ensure that the Executive Branch has sufficient time in an emergency situation to prepare an application, obtain the required approvals of senior officials, apply for a Court order, and satisfy the court that the

application should be granted. I note that this extension, if granted, would not change the substantive findings required before emergency authorization may be obtained. In all circumstances, prior to the Attorney General authorizing emergency electronic surveillance or physical search pursuant to FISA, the Attorney General must make a finding that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. Extending the time periods to prepare applications after this authorization would not affect the findings the Attorney General is currently required to make.

These changes would substantially improve the bureaucratic processes involved in preparing FISA applications, without affecting the important substantive requirements of the law.

Mr. Chairman, this concludes my remarks.

Mr. CONYERS. I thank you very much.

And we now turn to the Assistant Attorney General for National Security, Mr. Kenneth Wainstein.

Welcome.

TESTIMONY OF KENNETH L. WAINSTEIN, ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY, UNITED STATES DEPARTMENT OF JUSTICE

Mr. WAINSTEIN. Thank you, Chairman Conyers, Members of the Committee. Thank you very much for this opportunity to testify concerning FISA modernization.

I am proud to be here to represent the Department of Justice and to have the opportunity to discuss this very important issue with you.

I would like to just take a few moments here to explain why it is I think that we need to make the protect act permanent. And to do that, I would like to go through my understanding of the history and the evolution of the FISA statute.

In enacting FISA, the Congress of 1978 was reacting to the abuses that had been disclosed in the Church and Pike hearings that involved surveillance against Americans within America.

And they reacted by establishing a regime of judicial review for foreign intelligence surveillance activities, but not for all such activities, only for those that most substantially implicated the privacy interests of people in the United States.

Congress designed a judicial review process that would apply primarily to surveillance activities within the United States where privacy interests are most pronounced and not to overseas surveillance against foreign targets, where cognizable privacy interests are minimal or nonexistent.

Congress gave effect to this careful balancing through its definition of the statutory term "electronic surveillance," which is sort of the gatekeeper term in the statute that identifies those Government activities that fall within the scope of the statute and, by implication, those that fall outside the scope of the statute.

And Congress established this dichotomy by defining electronic surveillance by reference to the manner of communication under surveillance.

As the director said, by distinguishing between wire communications, which at that time included most of the local and domestic traffic, and were largely brought within the scope of the statute—distinguishing between them and radio communications, which included most of the transoceanic traffic of the time, and were largely left outside the scope of the statute.

And based on the communications reality of that era, that dichotomy more or less accomplished what it was that Congress intended to do, which was to distinguish between domestic communications that generally fell within FISA and foreign international communications that generally did not.

As the director said, however, the revolution in communications technology since that time radically altered that realty and upset the careful balance that was crafted in the statute.

And as a result, certain surveillance activities directed at persons overseas that were not intended to be within FISA became subject

to FISA, requiring us to go to get court authorizations before initiating surveillance and effectively conferring quasi-Constitutional protections on terrorist suspects and other national security targets overseas.

In April of this year, the Administration submitted to Congress a comprehensive proposal that would remedy this problem and provide a number of important refinements to the FISA statute.

While Congress has yet to act on the complete package we submitted, your passage of the temporary legislation in August was a significant step in the right direction.

That legislation updated the definition of electronic surveillance to exclude surveillance directed at persons reasonably believed to be outside the U.S., thereby restoring FISA to its original focus on domestic surveillance.

By making this change, Congress enabled the intelligence community to close critical intelligence gaps, and the Nation is already safer for it.

But the legislation only lasts for 6 months, and the new authority is scheduled to expire on February 5, absent reauthorization.

We urge Congress to make the Protect America Act permanent and to enact the other important FISA reforms contained in the package we submitted in April.

It is particularly imperative that Congress provide liability protection to companies that are alleged to have assisted the Nation in the conduct of intelligence activities in the wake of the September 11 attacks.

I see this renewal period from now until February as an opportunity to do two things. First and foremost, it gives us, the United States government, the opportunity to demonstrate that we can use this authority both effectively and responsibly. And this is an opportunity that we have already started to seize.

As we explained in a letter we sent this Committee back on September 5, we have already established a strong regime of oversight for this authority, which includes regular internal agency audits as well as on-site compliance reviews by a team from the Office of the Director of National Intelligence and the National Security Division in the Department of Justice.

In that same letter, we also committed to providing Congress with comprehensive reports about how we are implementing this authority. We will make ourselves available to brief you and your staffs regularly on our compliance reviews and what we find.

We will provide you copies of the written reports of those reviews, and we will give you update briefings every month on compliance matters and the implementation of this authority in general.

And we are confident that this regime of oversight and congressional reporting will establish a solid track record for our use of this authority.

This interim period also gives us one other opportunity, and that is the opportunity to engage in a serious debate and dialogue on this important issue.

I feel strongly that American liberty and security were advanced by this act and that they will be further advanced by adoption of our comprehensive FISA modernization proposal.

However, I recognize that this is a matter of significant and legitimate concern to many throughout the country.

On Friday we sent the Committee a letter that addressed some of the common concerns about the act, and we hope that that letter provides further assurances to Congress and the American people that the act is a measured and sound approach to an important intelligence challenge.

This Committee is very wise to be holding this hearing today and to explore the various legislative options and their implications for national security and civil liberties.

I am confident that when those options and implications are subject to objective scrutiny and honest debate, Congress and the American people will see both the wisdom and the critical importance of modernizing the FISA statute on a permanent basis.

Thank you again, Mr. Chairman, for allowing me to appear before you, and I look forward to answering your questions.

[The prepared statement of Mr. Wainstein follows:]

PREPARED STATEMENT OF THE HONORABLE KENNETH L. WAINSTEIN

STATEMENT OF
KENNETH L. WAINSTEIN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

BEFORE THE

COMMITTEE ON THE JUDICIARY

SEPTEMBER 18, 2007

Chairman Conyers, Ranking Member Smith, and Members of the Committee, thank you for this opportunity to testify concerning the modernization of the Foreign Intelligence Surveillance Act of 1978 (more commonly referred to as "FISA").

As you are aware, Administration officials have testified repeatedly over the last year regarding the need to modernize FISA. In April of this year, the Director of National Intelligence (DNI) submitted to Congress a comprehensive proposal to modernize the statute. The DNI, the Director of the National Security Agency (NSA), the general counsels of ODNI and NSA, and I testified before the Senate Select Committee on Intelligence regarding that proposal in May. The Department of Justice continues to support permanently and comprehensively modernizing FISA in accordance with the Administration's proposal. While I commend Congress for passing the Protect America Act of 2007 (the "Protect America Act") in August, the Act is a partial solution that will expire in less than six months. We urge the Congress to make the Protect America Act permanent, and also to enact the other important reforms to FISA contained in the Administration's proposal. It is especially imperative that

Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. By permanently modernizing and streamlining FISA, we can improve our efforts to gather intelligence on those who seek to harm us, and do so in a manner that protects the civil liberties of Americans.

In my testimony today, I will briefly summarize the primary reasons that FISA needs to be updated. I will then discuss the implementation of the Protect America Act and address several concerns and misunderstandings that have arisen regarding the Act. Finally, to ensure the Committee has a detailed explanation of the Administration's proposal, I have included a section by section analysis of the legislation.

The Need for Permanent FISA Modernization

To understand why FISA needs to be modernized, it is important to understand some of the historical background regarding the statute. Congress enacted FISA in 1978 for the purpose of establishing a "statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes."[1] The law authorized the Attorney General to make an application to a newly established court -- the Foreign Intelligence Surveillance Court (or "FISA Court") -- seeking a court order approving the use of "electronic surveillance" against foreign powers or their agents.

The law applied the process of judicial approval to certain surveillance activities (almost all of which occur within the United States), while excluding from FISA's regime of court supervision the vast majority of overseas foreign intelligence surveillance activities, including most surveillance focused on foreign targets. The intent of Congress generally to exclude these intelligence activities from FISA's reach is expressed clearly in the House Permanent Select Committee on Intelligence's report, which explained: "[t]he committee has explored the

[1] H.R. Rep. No. 95-1283, pt. 1, at 22 (1978).

feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances."[2]

The mechanism by which Congress gave effect to this intent was its careful definition of "electronic surveillance," the term that identifies which Government activities fall within FISA's scope. This statutory definition is complicated and difficult to parse, in part because it defines "electronic surveillance" by reference to particular communications technologies that were in place in 1978. (Indeed, as will be explained shortly, it is precisely FISA's use of technology-dependent provisions that has caused FISA to apply to activities today that its drafters never intended.)

The original definition of electronic surveillance is the following:

> (f) "Electronic surveillance" means-
>
> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
>
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
>
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from

[2] *Id.* at 27.

> a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.[3]

This definitional language is fairly opaque at first glance, and it takes some analysis to understand its scope. Consider at the outset the first part of the definition of electronic surveillance, which encompasses the acquisition of "the contents of any wire or radio communication sent by or intended to be received by *a particular, known United States person who is in the United States*, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." The point of this language is fairly clear: if the Government intentionally targets a particular, known U.S. person in the United States for foreign intelligence surveillance purposes, it is within FISA's scope, period.

Further analysis of that definitional language also demonstrates the opposite—that surveillance targeting someone overseas was generally <u>not</u> intended to be within the scope of the statute. This conclusion is evidenced by reference to the telecommunications technologies that existed at the time FISA was enacted. In 1978, almost all transoceanic communications into and out of the United States were carried by satellite, which qualified as "radio" (vs. "wire") communications. Under the statutory definition, surveillance of these international/"radio" communications would become "electronic surveillance" only if either (i) the acquisition intentionally targeted a U.S. person in the United States (in which case the acquisition would have fallen within the scope of the first definition of "electronic surveillance");[4] or (ii) *all* of the participants to the communication were located in the United States (which would satisfy the third definition of electronic surveillance, i.e. that "both the sender and all intended recipients are

[3] 50 U.S.C. 1801 (f).
[4] 50 U.S.C. 1801 (f)(1).

in the United States").[5] Therefore, if the Government in 1978 acquired communications by targeting a foreign person overseas, it usually was not engaged in "electronic surveillance" and the Government did not have to go to the FISA Court for an order authorizing that surveillance. This was true even if one of the communicants was in the United States.

As satellite ("radio") gave way to transoceanic fiber optic cables ("wire") for the transmission of most international communications and other technological advances changed the manner of international communications, the scope of activities covered by FISA expanded -- without any conscious choice by Congress -- to cover a wide range of intelligence activities that Congress intended to exclude from FISA in 1978. This unintended expansion of FISA's scope hampered our intelligence capabilities and caused us to expend resources on obtaining court approval to conduct intelligence activities directed at foreign persons overseas. Prior to the passage of the Protect America Act of 2007, the Government often needed to obtain a court order before intelligence collection could begin against a target located overseas. Thus, considerable resources of the Executive Branch and the FISA Court were being expended on obtaining court orders to monitor the communications of terrorist suspects and other national security threats abroad. This effectively was granting quasi-constitutional protections to these foreign terrorist suspects, who frequently are communicating with other persons outside the United States.

In certain cases, this process of obtaining a court order slowed, and in some cases may have prevented, the Government's efforts to conduct surveillance of communications that were potentially vital to the national security. This expansion of FISA's reach also necessarily

[5] At the time of FISA's enactment, the remaining two definitions of "electronic surveillance" did not implicate most transoceanic communications. The first of these definitions, in section 1801(f)(2), applied only to "wire communications," which in 1978 carried a comparatively small number of transoceanic communications. The second definition, in section 1801(f)(4), was a residual definition that FISA's drafters explained was "not meant to include . . . the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States." H.R. Rep. No. 95-1283 at 52.

diverted resources that would have been better spent on protecting the privacy interests of United States persons here in the United States.

The legislative package we submitted in April proposed to fix this problem by amending the definition of "electronic surveillance" to focus on *whose* communications are being monitored, rather than on *how* the communications travels or *where* they are being intercepted. No matter the mode of communication (radio, wire or otherwise) or the location of interception (inside or outside the United States), if a surveillance is directed at a person in the United States, FISA generally should apply; if a surveillance is directed at persons overseas, it should not. This fix was intended to provide the Intelligence Community with much needed speed and agility while, at the same time, refocusing FISA's privacy protections on persons located in the United States.

The Protect America Act of 2007

Although Congress has yet to conclude its consideration of the Administration's proposal, you took a significant step in the right direction by passing the Protect America Act last month. We urge Congress to make the Act permanent and to enact other important reforms to FISA contained in the Administration's proposal. It is particularly critical that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks.

By updating the definition of "electronic surveillance" to exclude surveillance directed at persons reasonably believed to be outside the United States, the Protect America Act clarified that FISA does not require a court order authorizing surveillance directed at foreign intelligence targets located in foreign countries. This law has temporarily restored FISA to its original, core purpose of protecting the rights and liberties of people in the United States, and the Act allows

the Government to collect the foreign intelligence information necessary to protect our nation.

Under section 105B of the Act, if targets are reasonably believed to be located outside the United States, the Attorney General and the DNI jointly may authorize the acquisition of foreign intelligence information without a court order if several statutory requirements are met. For acquisitions pursuant to section 105B, among other requirements, the Attorney General and the DNI must certify that reasonable procedures are in place for determining that the acquisition concerns persons reasonably believed to be outside the United States, that the acquisition does not constitute "electronic surveillance," and that the acquisition involves obtaining the information from or with the assistance of a communications service provider, custodian, or other person.

The Act permits the Attorney General and the DNI to direct persons to provide the information, facilities, and assistance necessary to conduct the acquisition, and the Attorney General may invoke the aid of the FISA Court to compel compliance with the directive. A person who receives such a directive also may seek review of the directive from the FISA Court. The Act also provides that no cause of action may be brought in any court against any person for complying with a directive.

While a court order is not required for the acquisition of foreign intelligence information regarding overseas targets under section 105B to begin, the FISA Court still is involved in reviewing the procedures utilized in acquisitions under that section. Under the Act, the Attorney General is required to submit to the FISA Court the procedures by which the Government determines that the authorized acquisitions of foreign intelligence information under section 105B concern persons reasonably believed to be outside the United States and therefore do not constitute electronic surveillance. The FISA Court then must review the Government's

determination that the procedures are reasonable and decide whether or not that determination is clearly erroneous.

The following is an overview of the implementation of this authority to date.

(1) Our Use of this New Authority

The authority provided by the Act is an essential one and allowed us effectively to close an intelligence gap identified by the DNI that was caused by FISA's outdated provisions.

(2) Oversight of this New Authority

As we explained in a letter we sent the leadership of this Committee on September 5, 2007, we have already established a strong regime of oversight for this authority and already have begun our oversight activities. This oversight includes:

- regular reviews by the internal compliance office of any agency that exercises authority given it under new section 105B of FISA;
- a review by the Department of Justice and ODNI, within fourteen days of the initiation of collection under this new authority, of an agency's use of the authority to assess compliance with the Act, including with the procedures by which the agency determines that the acquisition of foreign intelligence information concerns persons reasonably believed to be located outside the United States and with the applicable minimization procedures; and,
- subsequent reviews by the Department and ODNI at least once every 30 days.

The Department's compliance reviews will be conducted by attorneys of the National Security Division with experience in undertaking reviews of the use of FISA and other national security authorities, in consultation with the Department's Privacy and Civil Liberties Office, as appropriate, and ODNI's Civil Liberties Protection Office. Moreover, an agency using this authority will be under an ongoing obligation to report promptly to the Department and to ODNI incidents of noncompliance by its personnel.

(3) Congressional Reporting About Our Use of this New Authority

We intend to provide reporting to Congress about our implementation and use of this new authority that goes well beyond the reporting required by the Act. The Act provides that the Attorney General shall report on acquisitions under section 105B on a semiannual basis to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on the Judiciary of the Senate and of the House of Representatives. This report must include incidents of non-compliance with the procedures used to determine whether a person is reasonably believed to be located outside the United States, non-compliance by a recipient of a directive, and the number of certifications issued during the reporting period.

Because we appreciate the need for regular and comprehensive reporting during the debate of renewal of this authority, we are committing to substantial reporting beyond that required by the statute. As we explained in our September 5, 2007, letter, we will provide the following reports and briefings to Congress over the course of the six-month renewal period:

- we will make ourselves available to brief you and your staffs on the results of our first compliance review and after each subsequent review;
- we will make available to you copies of the written reports of those reviews, with redactions as necessary to protect critical intelligence sources and methods;
- we will give you update briefings every month on the results of further compliance reviews and generally on our use of the authority under section 105B; and,
- because of the exceptional importance of making the new authority permanent and of enacting the remainder of the Administration's proposal to modernize FISA, the Department will make appropriately redacted documents (accommodating the Intelligence Community's need to protect critical intelligence sources and methods) concerning implementation of this new authority available, not only to the Intelligence committees, but also to members of the Judiciary committees and to their staff with the necessary clearances.

As I stated above, we already have completed the first compliance review and are prepared to brief you on that review whenever it is convenient for you.

I am confident that this regime of oversight and congressional reporting will demonstrate that we are effectively using this new authority to defend our country while assiduously protecting the civil liberties and privacy interests of Americans.

(4) Concerns and Misunderstandings about the New Authority

I also want briefly to address some of the concerns and misunderstandings that have arisen regarding the Protect America Act. In response to a request from the Chairman and other members of the House Permanent Select Committee on Intelligence after a September 6, 2007, hearing, we sent a letter to that Committee that clearly outlines the position of the Executive Branch on several such issues. We also sent a copy of that letter to this Committee and we hope that the letter dispels any concerns or misunderstandings about the new law. In an effort to ensure the position of the Executive Branch is clear, I will reiterate our position on those issues in this statement.

First, some have questioned the Protect America Act's application to domestic communications and whether this authority could be used to circumvent the requirement for a FISA Court order to intercept communications within the United States. As noted above, the Act clarifies that FISA's definition of electronic surveillance does not "encompass surveillance directed at a person reasonably believed to be located *outside of the United States*," Protect America Act § 2, Pub. L. No. 110-55, 121 Stat. 52, 50 U.S.C. § 1805A (emphasis added), but this change does not affect the application of FISA to persons inside the United States. It leaves undisturbed FISA's definition of electronic surveillance as it applies to domestic-to-domestic communications and surveillance targeting persons located in the United States. In other words,

the Protect America Act leaves in place FISA's requirements for court orders to conduct electronic surveillance directed at persons in the United States.

Some have, nonetheless, suggested that language in the Protect America Act's certification provision in section 105B, which allows the Attorney General and the Director of National Intelligence to authorize the acquisition of certain information "concerning" persons outside the United States, gives us new latitude to conduct domestic surveillance. Specifically, they ask whether we can collect domestic-to-domestic communications or target a person inside the United States for surveillance on the theory that we are seeking information "concerning" persons outside the United States.

This concern about section 105B is misplaced because this provision must be read in conjunction with the pre-existing provisions of FISA. That section provides that it can be used only to authorize activities that are *not* "electronic surveillance" under FISA, *id.* at § 1805B(a)(2)—a definition that, as noted above, continues to apply as it did before to acquisition of domestic-to-domestic communications and to the targeting of persons within the United States. To put it plainly: The Protect America Act does not authorize so-called "domestic wiretapping" without a court order, and the Executive Branch will not use it for that purpose.

Second, some have questioned whether the Protect America Act authorizes the Executive Branch to conduct physical searches of the homes or effects of Americans without a court order. Several specific variations of this question were asked: Does the Act authorize physical searches of domestic mail without court order? Of the homes or businesses of foreign intelligence targets located in the United States? Of the personal computers or hard drives of individuals in the United States? The answer to each of these questions is "no." The statute does not authorize these activities.

Section 105B was intended to provide a mechanism for the government to obtain third-party assistance, *specifically in the acquisition of communications of persons located outside the United States*, and not in the physical search of homes, personal effects, computers or mail of individuals within the United States. That section only allows the Attorney General and the Director of National Intelligence to authorize activities that, among other limitations, involve obtaining foreign intelligence information "from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications." Protect America Act § 2, 50 U.S.C. § 1805B(a)(3).

Traditional canons of statutory construction dictate that "where general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words." 2A Sutherland, *Statutes and Statutory Construction*, § 47.17, at 188. The language of section 105B(a)(3) therefore is best read to authorize acquisitions only from or with the assistance of private entities that provide communications. That reading of the statute is reinforced by the requirement in section 105B(a)(3) that such entities have access to communications, either as they are transmitted or while they are stored, or equipment that is used or may be used to transmit or store such communications—further demonstrating that this section is limited to acquisitions from or with the assistance of entities that provide communications. It is therefore clear that the Act does not authorize physical searches of the homes, mail, computers and personal effects of individuals in the United States, and the Executive Branch will not use it for

such purposes.

Third, some have asked whether the Government will use section 105B to obtain the business records of individuals located in the United States. It should be noted that many of the limitations already referenced above would sharply curtail even the hypothetical application of section 105B to acquisitions of business records. For instance, the records would have to concern persons outside the United States; the records would have to be obtainable from or with the assistance of a communications service provider; and the acquisition could not constitute "electronic surveillance" under FISA. Protect America Act § 2, 50 U.S.C. § 1805B(a)(2)-(4). Therefore, this provision does not authorize the collection of (to cite just two examples) medical or library records for foreign intelligence purposes. And to the extent that this provision could be read to authorize the collection of business records of individuals in the United States on the theory that they "concern" persons outside the United States, we wish to make very clear that we will not use this provision to do so.

Fourth, some have expressed concerns that the Protect America Act authorizes so-called "reverse targeting" without a court order. It would be "reverse targeting" if the Government were to surveil a person overseas where the Government's actual purpose was to target a person inside the United States with whom the overseas person was communicating. The position of the Executive Branch has consistently been that such conduct would constitute "electronic surveillance" under FISA—because it would involve the acquisition of communications to or from a U.S. person in the United States "by intentionally targeting that United States person," 50 U.S.C. § 1801(f)(1)—and could not be conducted without a court order except under the specified circumstances set forth in FISA. This position remains unchanged after the Protect America Act, which excludes from the definition of electronic surveillance only surveillance

directed at targets overseas. Because it would remain a violation of FISA, the Government cannot—and will not—use this authority to engage in "reverse targeting."

It is also worth noting that, as a matter of intelligence tradecraft, there would be little reason to engage in "reverse targeting." If the Government believes a person in the United States is a terrorist or other agent of a foreign power, it makes little sense to conduct surveillance of that person by listening only to that subset of the target's calls that are to an overseas communicant whom we have under surveillance. Instead, under such circumstances the Government will want to obtain a court order under FISA to collect *all* of that target's communications.

Additionally, some critics of the new law have suggested that the problems the Intelligence Community has faced with FISA can be solved by carving out of FISA's scope only foreign to foreign communications. These critics argue that the Protect America Act fails adequately to protect the interests of people who communicate with foreign intelligence targets outside the United States, because there may be circumstances in which a foreign target may communicate with someone in the United States and that conversation may be intercepted. These critics would require the Intelligence Community to seek FISA Court approval any time a foreign target overseas happens to communicate with a person inside the United States. This is an unworkable approach, and I can explain the specific reasons why this approach is unworkable in a classified setting.

Requiring court approval when a foreign target happens to communicate with a person in the United States also would be inconsistent with the Intelligence Community's long-standing authority to conduct warrantless surveillance on suspects overseas pursuant to Executive Order 12333. There is no principled rationale for requiring a court order to surveil these suspects' communications when we intercept them in the United States when no court order is required for

surveilling those very same communications (including communications between those suspects and persons within the United States) when we happen to conduct the interception outside the United States. Moreover, it is not in the interest of either the national security or the civil liberties of Americans to require court orders for surveillance of persons overseas.

I also note that such an approach would be at odds with the law and practice governing the analogous situation in the criminal context. In the case of a routine court-ordered criminal investigation wiretap, the Government obtains a court order to conduct surveillance of a criminal suspect. During that surveillance, the suspect routinely communicates with other individuals for whom the Government has not obtained wiretap warrants and who are often completely innocent of any complicity in the suspected criminal conduct. Nonetheless, the Government may still monitor those conversations that are relevant, and it need not seek court authorization as to those other individuals. Instead, the Government addresses these communications through minimization procedures.

Similarly, Intelligence Community personnel should not be required to obtain a court order if they are lawfully surveilling an overseas target and that target happens to communicate with someone in the United States. Rather, like their law enforcement counterparts, they should simply be required to employ the minimization procedures they have employed for decades in relation to the communications they intercept pursuant to their Executive Order 12333 authority. As this Committee is aware, the Intelligence Community employs careful and thorough minimization procedures to handle the acquisition, dissemination, and retention of incidentally collected U.S. person information in the foreign intelligence arena. As Congress recognized in 1978, these rigorous procedures are a far more workable approach to protecting the privacy interests of Americans communicating with a foreign target than a sweeping new regime of

judicial supervision for foreign intelligence surveillance activities targeting foreign persons overseas.

Finally, some have asked why we cannot simply maintain the pre-Protect America Act status quo and simply commit more resources to handle the workload. Committing more resources and manpower to the production of FISA applications for overseas targets is not the silver bullet. The Department of Justice, the NSA and the other affected agencies will always have finite resources, and resources committed to tasks that have little bearing on cognizable privacy interests are resources that cannot be committed to tasks that do. And additional resources will not change the fact that it makes little sense to require a showing of probable cause to surveil a terrorist overseas -- a showing that will always require time and resources to make. The answer is not to throw money and personnel at the problem; the answer is to fix the problem in the first place.

In sum, the Protect America Act was a good decision for America, and one that is greatly appreciated by those of us who are entrusted with protecting the security of the nation and the liberties of our people.

The FISA Modernization Proposal

While the Protect America Act temporarily fixed one troubling aspect of FISA, the statute needs to be permanently and comprehensively modernized. First, the Protect America Act should be made permanent. Second, Congress should provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. Third, it is important that Congress consider and ultimately pass other provisions in our proposal. These provisions -- which draw from a number of thoughtful bills introduced in Congress during its last session -- would make a number of

salutary improvements to the FISA statute. Among the most significant are the following:

- The proposal would amend the statutory definition of "agent of a foreign power" -- a category of individuals the Government may target with a FISA court order -- to include groups and individuals involved in the international proliferation of weapons of mass destruction. There is no greater threat to our nation than that posed by those who traffic in weapons of mass destruction, and this amendment would enhance our ability to identify, investigate and incapacitate such people before they cause us harm.

- The bill would provide a mechanism by which third parties -- primarily telecommunications providers -- could challenge a surveillance directive in the FISA Court.

- The bill would also streamline the FISA application process in a manner that will make FISA more efficient, while at the same time ensuring that the FISA Court has the essential information it needs to evaluate a FISA application.

These and other sections of the proposal are detailed in the following section-by-section analysis.

Section by Section Analysis

The Protect America Act temporarily restored FISA to its original and core purpose of protecting the rights of liberties of people in the United States. The Act achieved some of the goals the Administration sought in the proposal it submitted to Congress in April and we believe the Act should be made permanent. Additionally, it is critical that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. This important provision is contained in section 408 of our proposal. For purposes of providing a complete review of the legislation proposed by the Administration in April, the following is a short summary of each proposed change in the bill -- both major and minor. This summary includes certain provisions that would not be necessary if the Protect America Act is made permanent.

Section 401

Section 401 would amend several of FISA's definitions to address the consequences of the changes in technology that I have discussed. Most importantly, subsection 401(b) would redefine the term "electronic surveillance" in a technology-neutral manner that would refocus FISA on the communications of individuals in the United States As detailed above, when FISA was enacted in 1978, Congress used language that was technology-dependent and related specifically to the telecommunications systems that existed at that time. As a result of revolutions in communications technology since 1978, and not any considered judgment of Congress, the current definition of "electronic surveillance" sweeps in surveillance activities that Congress actually intended to *exclude* from FISA's scope. In this manner, FISA now imposes an unintended burden on intelligence agencies to seek court approval for surveillance in circumstances outside the scope of Congress' original intent.

Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should this Congress. A technology-neutral statute would prevent the type of unintended consequences we have seen and it would provide a lasting framework for electronic surveillance conducted for foreign intelligence purposes. Thus, FISA would no longer be subject to unforeseeable technological changes. We should not have to overhaul FISA each generation simply because technology has changed.

Subsection 401(b) of our proposal provides a new, technology-neutral definition of "electronic surveillance" focused on the core question of *who* is the subject of the surveillance, rather than on *how* or *where* the communication is intercepted. Under the amended definition, "electronic surveillance" would encompass: "(1) the installation or use of an electronic, mechanical, or other surveillance device for acquiring information by intentionally directing

surveillance at a particular, known person who is reasonably believed to be located within the United States under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or (2) the intentional acquisition of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the sender and all intended recipients are reasonably believed to be located within the United States." Under this definition, FISA's scope would not be defined by substantively irrelevant criteria, such as the means by which a communication is transmitted, or the location where the communication is intercepted. Instead, the definition would focus FISA's scope—as we believe Congress intended when it enacted the law in 1978—on those intelligence activities that most substantially implicate the privacy interests of persons in the United States.

Section 401 would make changes to other definitions in FISA as well. In keeping with the preference for technological neutrality, we would eliminate the distinction between "wire" and "radio" communications that appears throughout the Act. Accordingly, the Administration's proposal would strike FISA's current definition of "wire communication," because reference to that term is unnecessary under the new, technology neutral definition of "electronic surveillance."

The proposal also would amend other definitions to address gaps in FISA's coverage. Subsection 401(a) would amend FISA's definition of "agent of a foreign power" to include non-United States persons who possess or receive significant foreign intelligence information while in the United States. This amendment would ensure that the United States Government can collect necessary information possessed by a non-United States person visiting the United States. The amendment would thereby improve the Intelligence Community's ability to collect valuable

foreign intelligence in circumstances where a non-United States person in the United States is known to the United States Government to possess valuable foreign intelligence information, but his relationship to a foreign power is unclear. I can provide examples in which this definition would apply in a classified setting. It merits emphasis that the Government would still have to obtain approval from the FISA Court to conduct surveillance under these circumstances.

Section 401 also amends the definition of the term "minimization procedures." This is an amendment that would be necessary to give meaningful effect to a proposed amendment to 50 U.S.C. 1802(a), discussed in detail below. Finally, section 401 would make the FISA definition of the term "contents" consistent with the definition of "contents" as that term is used in Title III, which pertains to interception of communications in criminal investigations. The existence of different definitions of "contents" in the intelligence and law enforcement contexts is confusing to those who must implement the statute.

Section 402

Section 402 would accomplish several objectives. First, it would alter the circumstances in which the Attorney General can exercise his authority – present in FISA since its passage – to authorize electronic surveillance without a court order. Currently, subsection 102(a) of FISA allows the Attorney General to authorize electronic surveillance without a court order where the surveillance is "solely directed" at the acquisition of the contents of communications "transmitted by means of communications used *exclusively*" between or among certain types of traditional foreign powers. This exclusivity requirement was logical thirty years ago in light of the manner in which certain foreign powers communicated at that time. But the means by which these foreign powers communicate has changed over time, and these changes in communications technology have seriously eroded the applicability and utility of current section 102(a) of FISA.

As a consequence, the Government must generally seek FISA Court approval for the same sort of surveillance today.

It is important to note that the proposed amendment to this provision of FISA would not alter the types of "foreign powers" to which this authority applies. It still would apply only to foreign Governments, factions of foreign nations (not substantially composed of United States persons), and entities openly acknowledged by a foreign Government to be directed and controlled by a foreign Government or Governments. Moreover—and this is important when read in conjunction with the change to the definition of "minimization procedures" referenced in section 401—any communications involving United States persons that are intercepted under this provision still will be handled in accordance with minimization procedures that are equivalent to those that govern court-ordered collection.

Section 402 also would create new procedures (those proposed in new sections 102A and 102B) pursuant to which the Attorney General could authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States, under circumstances in which the acquisition does not constitute "electronic surveillance" under FISA. This is a critical change that works hand in glove with the new definition of "electronic surveillance" in section 401. FISA currently provides a mechanism for the Government to obtain a court order compelling communications companies to assist in conducting electronic surveillance. Because the proposed legislation would reduce the scope of the definition of "electronic surveillance," certain activities that previously were "electronic surveillance" under FISA would fall out of the statute's scope. This new provision would provide a mechanism for the Government to obtain the aid of a court to ensure private sector cooperation with these lawful intelligence activities no longer covered by the definition of "electronic surveillance." The new

section would also provide a means for third parties receiving such a directive to challenge the legality of that directive in court.

Section 403

Section 403 makes two relatively minor amendments to FISA. First, subsection 403(a) amends section 103(a) of FISA to provide that judges on the FISA Court shall be drawn from "at least seven" of the United States judicial circuits. The current requirement – that judges be drawn from seven different judicial circuits – unnecessarily complicates the designation of judges for that important court.

Subsection 403(b) also moves to section 103 of FISA, with minor amendments, a provision that currently appears in section 102. New section 103(g) would provide that applications for a court order under section 104 of FISA are authorized if the Attorney General approves the applications to the FISA Court, and a judge to whom the application is made may grant an order approving electronic surveillance in accordance with the statute—a provision that is most suitably placed in section 103 of FISA, which pertains to the FISA Court's jurisdiction. The new provision would eliminate the restriction on the FISA Court's jurisdiction in 50 U.S.C. § 1802(b), which provides that the court cannot grant an order approving electronic surveillance directed at the types of foreign powers described in section 102(a) unless the surveillance may involve the acquisition of communications of a United States person. Although the Government still would not be required to obtain FISA Court orders for surveillance involving those types of foreign powers, the removal of this restriction would permit the Government to seek FISA Court orders in those circumstances when an order is desirable.

Section 404

The current procedure for applying to the FISA Court for a surveillance order under

section 104 of FISA should be streamlined. While FISA should require the Government to provide information necessary to establish probable cause and other essential FISA requirements, FISA today requires the Government to provide information that is not necessary to these objectives.

Section 404 would attempt to increase the efficiency of the FISA application process in several ways. First, the Government currently is required to provide significant amounts of information that serves little or no purpose in safeguarding civil liberties. By amending FISA to require only summary descriptions or statements of certain information, the burden imposed on applicants for a FISA Court order authorizing surveillance will be substantially reduced. For example, section 404 would amend the current FISA provision requiring that the application contain a "detailed description of the nature of the information sought," and would allow the Government to submit a summary description of such information. Section 404 similarly would amend the current requirement that the application contain a "statement of facts concerning all previous applications" involving the target, and instead would permit the Government to provide a summary of those facts. While these amendments would help streamline FISA by reducing the burden involved in providing the FISA Court with information that is not necessary to protect the privacy of U.S. persons in the United States, the FISA Court would still receive the information it needs in considering whether to authorize the surveillance.

Section 404 also would increase the number of individuals who can make FISA certifications. Currently, FISA requires that such certifications be made only by senior Executive Branch national security officials who have been confirmed by the Senate. The new provision would allow certifications to be made by individuals specifically designated by the President and would remove the restriction that such individuals be Senate-confirmed. As this

committee is aware, many intelligence agencies have an exceedingly small number of Senate-confirmed officials (sometimes only one, or even none), and the Administration's proposal would allow intelligence agencies to more expeditiously obtain certifications.

Section 405

Section 405 would amend the procedures for the issuance of an order under section 105 of FISA to conform with the changes to the application requirements that would be effected by changes to section 104 discussed above.

Section 405 also would extend the initial term of authorization for electronic surveillance of a non-United States person who is an agent of a foreign power from 120 days to one year. This change will reduce time spent preparing applications for renewals relating to non-United States persons, thereby allowing more resources to be devoted to cases involving United States persons. Section 405 would also allow any FISA order to be extended for a period of up to one year. This change would reduce the time spent preparing applications to renew FISA orders that already have been granted by the FISA Court, thereby increasing the resources focused on initial FISA applications.

Additionally, section 405 would make important amendments to the procedures by which the Executive Branch may initiate emergency authorizations of electronic surveillance prior to obtaining a court order. Currently the Executive Branch has 72 hours to obtain court approval after emergency surveillance is initially authorized by the Attorney General. The amendment would extend the emergency period to seven days. This change will help ensure that the Executive Branch has sufficient time in an emergency situation to accurately prepare an application, obtain the required approvals of senior officials, apply for a court order, and satisfy the court that the application should be granted. This provision also would modify the existing

provision that allows certain information to be retained when the FISA Court rejects an application to approve an emergency authorization. Presently, such information can be retained if it indicates a threat of death or serious bodily harm to any person. The proposed amendment would also permit such information to be retained if the information is "significant foreign intelligence information" that, while important to the security of the country, may not rise to the level of death or serious bodily harm.

Finally, section 405 would add a new paragraph that requires the FISA Court, when granting an application for electronic surveillance, to simultaneously authorize the installation and use of pen registers and trap and trace devices if such is requested by the Government. This is a technical amendment that results from the proposed change in the definition of "contents" in Title I of FISA. And, of course, as the standard to obtain a court order for electronic surveillance is substantially higher than the pen-register standard, there should be no objection to an order approving electronic surveillance that also encompasses pen register and trap and trace information.

Section 406

Section 406 would amend subsection 106(i) of FISA, which pertains to limitations regarding the use of unintentionally acquired information. Currently, subsection 106(i) provides that lawfully but unintentionally acquired *radio* communications between persons located in the United States must be destroyed unless the Attorney General determines that the communications indicate a threat of death or serious bodily harm. Section 406 amends subsection 106(i) by making it technology-neutral; we believe that the same rule should apply regardless how the communication is transmitted. The amendment also would allow for the retention of unintentionally acquired information if it "contains significant foreign intelligence

information." This ensures that the Government can retain and act upon valuable foreign intelligence information that is collected unintentionally, rather than being required to destroy all such information that does not fall within the current exception.

Section 406 also would clarify that FISA does not preclude the Government from seeking protective orders or asserting privileges ordinarily available to protect against the disclosure of classified information. This is necessary to clarify any ambiguity regarding the availability of such protective orders or privileges in litigation.

Section 407

Section 407 would amend sections 101, 106, and 305 of FISA to address concerns related to weapons of mass destruction. These amendments reflect the threat posed by these catastrophic weapons and would extend FISA to apply to individuals and groups engaged in the international proliferation of such weapons. Subsection 407(a) amends section 101 of FISA to include a definition of the term "weapon of mass destruction." Subsection 407(a) also amends the section 101 definitions of "foreign power" and "agent of a foreign power" to include groups and individuals (other than U.S. persons) engaged in the international proliferation of weapons of mass destruction. Subsection 407(a) similarly amends the definition of "foreign intelligence information." Finally, subsection 407(b) would amend sections 106 and 305 of FISA, which pertain to the use of information, to include information regarding the international proliferation of weapons of mass destruction.

Section 408

Section 408 would provide litigation protections to telecommunications companies who are alleged to have assisted the Government with classified communications intelligence activities in the wake of the September 11th terrorist attacks. Telecommunications companies

have faced numerous lawsuits as a result of their alleged activities in support of the Government's efforts to prevent another terrorist attack. If private industry partners are alleged to cooperate with the Government to ensure our nation is protected against another attack, they should not be held liable for any assistance they are alleged to have provided.

Section 409

Section 409 would amend section 303 of FISA (50 U.S.C. 1823), which relates to physical searches, to streamline the application process, update and augment the emergency authorization provisions, and increase the potential number of officials who can certify FISA applications. These changes largely parallel those proposed to the electronic surveillance application process. For instance, they include amending the procedures for the emergency authorization of physical searches without a court order to allow the Executive Branch seven days to obtain court approval after the search is initially authorized by the Attorney General. Section 409 also would amend section 304 of FISA, pertaining to orders authorizing physical searches, to conform to the changes intended to streamline the application process.

Additionally, section 409 would permit the search of not only property that *is* owned, used, possessed by, or in transit to or from a foreign power or agent of a foreign power, but also property that is *about* to be owned, used, possessed by, or in transit to or from these powers or agents. This change makes the scope of FISA's physical search provisions coextensive with FISA's electronic surveillance provisions in this regard.

Section 410

Section 410 would amend the procedures found in section 403 of FISA (50 U.S.C. 1843) regarding the emergency use of pen registers and trap and trace devices without court approval to allow the Executive Branch seven days to obtain court approval after the emergency use is

initially authorized by the Attorney General. (The current period is 48 hours.) This change would ensure the same flexibility for these techniques as would be available for electronic surveillance and physical searches.

Section 411

Section 411 would allow for the transfer of sensitive national security litigation to the FISA Court in certain circumstances. This provision would require a court to transfer a case to the FISA Court if: (1) the case is challenging the legality of a classified communications intelligence activity relating to a foreign threat, or the legality of any such activity is at issue in the case, and (2) the Attorney General files an affidavit under oath that the case should be transferred because further proceedings in the originating court would harm the national security of the United States. By providing for the transfer of such cases to the FISA Court, section 411 ensures that, if needed, judicial review may proceed before the court most familiar with communications intelligence activities and most practiced in safeguarding the type of national security information involved. Section 411 also provides that the decisions of the FISA Court in cases transferred under this provision would be subject to review by the FISA Court of Review and the Supreme Court of the United States.

Other Provisions

Section 412 would make technical and conforming amendments to sections 103, 105, 106, and 108 of FISA (50 U.S.C. 1803, 1805, 1806, 1808).

Section 413 provides that these amendments shall take effect 90 days after the date of enactment of the Act, and that orders in effect on that date shall remain in effect until the date of expiration. It would allow for a smooth transition after the proposed changes take effect.

Section 414 provides that any provision in sections 401 through 414 held to be invalid or

unenforceable shall be construed so as to give it the maximum effect permitted by law, unless doing so results in a holding of utter invalidity or unenforceability, in which case the provision shall be deemed severable and shall not affect the remaining sections.

Conclusion

While the Protect America Act temporarily addressed some of the issues we have faced with FISA's outdated provisions, it is essential that Congress modernize FISA in a comprehensive and permanent manner. The Protect America Act is a good start, but it is only a start. In addition to making the Protect America Act permanent, Congress should reform FISA in accordance with the other provisions in the proposal that the Administration submitted to the Congress in April. It is especially imperative that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. These changes would permanently restore FISA to its original focus on the protection of the privacy interests of Americans, improve our intelligence capabilities, and ensure that scarce Executive Branch and judicial resources are devoted to the oversight of intelligence activities that most clearly implicate the interests of Americans. We look forward to working with the Congress to achieve these critical goals.

Thank you for the opportunity to appear before you and testify in support of the Administration's proposal. I look forward to answering your questions.

Mr. CONYERS. Thank you, Mr. Wainstein.

Director McConnell, you have stated publicly that only 100 or less Americans have been targeted for foreign intelligence surveillance.

But that doesn't tell us how many have been, have had their phone calls overheard as a result of spying, whether they were targeted or not. Can you clear up that distinction for me?

And secondly, there is a provision here, well, the Department of Justice has taken the position that a person reasonably likely to be abroad means the target of a surveillance. Well, that is far from obvious in the language, and we want to codify this into a much more clear definition.

And finally, how can we proceed in this very important responsibility with which we are charged if we don't have the information and access to it about the Administration's surveillance programs both past and present?

We have been waiting a long time for that information, and it seems to me that it is a prerequisite to anything we are supposed to accomplish here. And I would like to get some public assurances over and above the private assurances you have given me about that subject.

And so if you can respond to those three observations, I will consider my time well spent.

Mr. MCCONNELL. Thank you for your question, Mr. Chairman. It gives me, actually, a chance to clarify my intent when I had an interview down in Texas, sitting beside the Chairman of my oversight committee, Congressman Reyes.

What I was attempting to do was respond to so much of the inaccuracy and claims and counterclaims that had been in the press, specifically, that we are spying on Americans, we have a broad drift net, and that sort of thing.

So I carefully considered making the comments at a summary level to provide some context and perspective of what this is really all about. And so what I chose to do was to provide some level of indication in terms of numbers about how this works.

I recall that before this was limited only to al-Qaida and related, and so the claim being that we are spying, you know, widely on all Americans—what I wanted to highlight was the targets are foreign, and when targets that are foreign——

Mr. CONYERS. Excuse the interruption.

Mr. MCCONNELL. Sir, no problem. When the targets are foreign, and we are targeting active terrorists that have an intent to carry out attacks in this country, the vast majority of that is foreign to foreign. On some occasion there would be a call into the United States.

Now, the law says—it did before and it still says—that if someone in the United States is the subject of surveillance, we must have a court order.

So what I tried to provide in those numbers is out of the thousands of things that we do in an overseas foreign context, what had resulted in a court order where we actually conducted some surveillance against a U.S. person—and that doesn't necessarily mean a U.S. citizen, but a U.S. person—in the United States numbered in the range of 100. That was what I was attempting to clarify.

Mr. CONYERS. Yes, but there are thousands that—I don't know how many else have been—that weren't targeted that have been tapped. That is what I am trying to get to. What is the answer?

Mr. MCCONNELL. Sir, there is confusion over what means—the word "tapped" means. When you target someone in the business that we are in, you can only target one end of a conversation. So in the context of doing our business, the target is foreign. The objective is foreign. The purpose is foreign intelligence.

So——

[Audience outburst.]

Mr. LUNGREN. Mr. Chairman, can we have regular order? There are people in the audience who are waiting to put their signs up. They do one after the other.

And I would ask that we have regular order—that anybody who puts a sign up be removed immediately and those who have signs sitting in their laps either be removed or have their signs removed.

There are a whole group of them in the second row from the back on the left side as I look at it. And this is unfair and is not the kind of hearing I know you wish to conduct when we are trying in this Committee to consider very serious matters.

Mr. CONYERS. And in addition, it is counterproductive.

Would the young lady that just put the sign up please excuse herself?

Now, if we have to clear the room—I mean, I am not going to tolerate—we are working under a very serious time restraint. There are going to be votes coming up. I have got 30 Members that want questions answered.

And I am not in a mood to tolerate the seriatim interruptions that are going on. And I hope that we can work cooperatively.

We want everybody interested in hearing the testimony and the Members' questions to join us in this room. But this is not a place for demonstrations, rallies or protests.

Excuse me.

Mr. MCCONNELL. Sir, what I was attempting to explain is when you are conducting surveillance in the context of electronic surveillance, you can only target one end of a conversation.

So you have no control over who that number might call or who they might receive a call from.

The reference I made to the joint commission earlier was someone in the United States, a target, a terrorist, calling out to a terrorist. We should have gotten that intercept, and hopefully, if we had, it would have perhaps helped us prevent 9/11.

Mr. CONYERS. Well, the question, though, still remains: How many Americans have been wiretapped without a court order?

Mr. MCCONNELL. None.

Mr. CONYERS. Thank you.

Mr. MCCONNELL. There are no wiretaps against Americans without a court order. None. What we are doing is we target a foreign person in a foreign country.

If that foreign person calls into the United States, we have to do something with that call. The process is called minimization. It was in the law in 1978. It has been reviewed by the court. It is a part of the law. It is the way it is handled.

Mr. CONYERS. Mr. Chairman, let me put it like this. How many have been overheard? I mean, you have got minimization techniques. You wouldn't have it if somebody wasn't being overheard.

Mr. MCCONNELL. Sir, I don't have the exact number. I will be happy to try to get the number and provide it to you. I just don't know.

Mr. CONYERS. Well, that is very, very critical, Mr. Director.

Mr. MCCONNELL. It is a very small number considering that there are billions of transactions every day. So we look at it in the——

Mr. CONYERS. Well, would it be asking too much for this Committee, all cleared for top secret, to be given a briefing on it?

Mr. MCCONNELL. Sure, I would be happy to do that.

Mr. CONYERS. We have got to know.

Mr. MCCONNELL. I would be happy to do that. But, sir, I need to answer your question one more time. How many Americans' phones have been tapped without a court order, and it is none.

Mr. CONYERS. I trust you.

Mr. MCCONNELL. The law requires us to get a court order, and——

Mr. CONYERS. I trust you.

Mr. MCCONNELL [continuing]. What I am trying to——

Mr. CONYERS. But I have got to find this out. I mean, blowing these kind of answers back at me when this is a thing that is on the minds of most Americans in this country is not adequate.

Mr. MCCONNELL. Mr. Chairman, when I was being confirmed, when I went through on the Senate side, a number of the Members asked me, "You are former military. Do you have the gumption to speak truth to power?" And I sure hope I do.

And I have spoken truth to power in the executive branch, and I intend to speak truth to power in the legislative branch. You asked me the question, and I gave you the answer.

The law requires us to have a warrant if we target anybody in this country. It is as simple as that.

Mr. CONYERS. Well, just my last comment—well, then why did you agree with us and then go to the—when you got the White House call, your attitude changed 180 degrees? You think I can't notice that?

Mr. MCCONNELL. Sir, that was characterized in the press inappropriately.

Mr. CONYERS. Well, I wasn't using the press to characterize it. I was using what you told me and what happened after that communication.

Mr. MCCONNELL. Sir, my position on this did not change at all from when I came back in and I started to understand the issue last April until this moment.

When I talked with various Members of the Committee—now, here is the issue, and it is important for you to capture this—I had very simple criteria. There were three.

The criteria was do not require us to have a warrant for a foreign target in a foreign country. Allow us to have liability protection for the carriers. And I was asking you should require us to have a warrant if we do surveillance in this country.

And that was the philosophical underpinning of my argument. When we engaged in dialogue, the issue was there were drafts in the Administration. There were drafts on the Hill.

If you change a word or a phrase, because this bill is so complex, it can have unintended consequences later on in the bill in terms of shutting you down or so on.

So when I was asked to agree to something, I said philosophically I can agree, but let me see the words. And when we had a chance to actually review the words, we had to say we can't accept this and here is the reason.

So I was not directed by the White House to change my position. I did not change my position. And I would be happy to work with any of the wording in the current bill in a way where we both can see what it means and understand its full implications, and if there is a better way to phrase it, we are happy to engage and consider that.

Mr. CONYERS. Thank you.

The Chair recognizes the longest-serving Ranking Member on the Judiciary Committee, Dan Lungren.

Mr. LUNGREN. With an interruption of 16 years. Thank you very much, Mr. Chairman. I appreciate that.

Admiral McConnell, thank you very much for your service. I find you to be an honorable man who has served this country under both Democratic and Republican regimes and have no reason to question your dedication to service or your veracity.

Let me ask you this. There seems to be some confusion that I hope we can clear up.

It is my understanding that when you took over, you realized that a FISA court judge had made a decision that based on the then-current language of the law, which came in in 1978, that it now required you to go for warrants in circumstances where you hadn't gone for warrants when the law was first established. Is that true?

Mr. MCCONNELL. Yes, sir, that is true.

Mr. LUNGREN. And is it true that you attempted to work under the law as interpreted by the court and found that as a result of working under those restrictions you were, that is, your agency was prohibited from successfully targeting foreign conversations that otherwise you would have for looking into possible terrorist activity?

Mr. MCCONNELL. Yes, sir, that is true.

Mr. LUNGREN. And is it also true, Admiral, that merely saying that foreign-to-foreign communications would no longer require warrants did not get to the nut of the problem?

Mr. MCCONNELL. That is correct, sir.

Mr. LUNGREN. And is it also true that because of technology, the way it works, without going into anything that is classified, you specifically target an individual you reasonably believe to be a foreign target outside the United States?

Mr. MCCONNELL. Yes, sir.

Mr. LUNGREN. And do that without a warrant?

Mr. MCCONNELL. That is correct.

Mr. LUNGREN. And you cannot beforehand know with any degree of certainty whether that person is going to have some conversations into the United States.

Mr. MCCONNELL. That is correct.

Mr. LUNGREN. And if you were required—because of that possibility that there may be a conversation into the United States, a communication into the United States, you had to get a warrant in each and every case, it would be impossible for you to do the job you have been asked to do.

Mr. MCCONNELL. That is correct.

Mr. LUNGREN. And you say that because, in fact, it proved impossible to do the job you were supposed to do.

Mr. MCCONNELL. Yes, sir.

Mr. LUNGREN. And we were excluded from obtaining crucial terrorist-related information from targets overseas that under the reading of the 1978 law, under the technology that existed at that time, we would have been able to reach without a warrant.

Mr. MCCONNELL. That is correct.

Mr. LUNGREN. So that what you have attempted to do, and what we did in this law, was to use the same legal construct, which was to take outside of the requirement for warrants those kinds of communications that weren't anticipated to be protected by the fourth amendment, because they were directed at individuals who were foreign in foreign countries.

Mr. MCCONNELL. That is correct.

Mr. LUNGREN. And that because on occasion—and we are saying occasionally because compared to the number of communications we are talking about, these are occasional communications into the United States at the other end. You have devised a system of minimization which is basically the same minimization we use in criminal cases.

Mr. MCCONNELL. Yes, sir.

Mr. LUNGREN. And in criminal cases when we get a wiretap on a suspected mafia member, we target the mafia member, we target the particular means of communication he uses, not knowing ahead of time who he is going to communicate with in the future.

Mr. MCCONNELL. That is correct.

Mr. LUNGREN. And that on those occasions when he does communicate with someone that has nothing to do with his mafia connection, we minimize.

Mr. MCCONNELL. Minimize.

Mr. LUNGREN. And you are doing the same thing now.

Mr. MCCONNELL. Yes, sir.

Mr. LUNGREN. And you had experience minimizing when you were head of the NSA.

Mr. MCCONNELL. I did.

Mr. LUNGREN. And you feel an obligation both legally, morally and ethically to follow the strictures of the law there.

Mr. MCCONNELL. Yes, sir, I do.

Mr. LUNGREN. And so when you tell us that you haven't wiretapped any individual in the United States without a warrant, you were saying you haven't targeted them as the individual from which you are seeking information.

You are not saying that you didn't pick up inadvertently conversations that came into the United States, correct?

Mr. MCCONNELL. That is correct.

Mr. LUNGREN. And when you did, you applied minimization, as we do on the criminal side, as we have been doing for 30 years or 50 years.

Mr. MCCONNELL. And if they were a target of interest, then that would mean we would have to now get a warrant if it was someone in the United States.

Mr. LUNGREN. And that is still the case.

Mr. MCCONNELL. That is still the case.

Mr. LUNGREN. And as I understand it, there is some concern that the new language could reach domestic-to-domestic communications or target a person inside the U.S. for surveillance—at least, this is what some of the critics have said—because that information is being sought "concerning persons outside the U.S."

If that criticism were true, it would have to mean that we are not looking at the preexisting language of FISA defining electronic surveillance, correct?

Mr. MCCONNELL. That is correct, sir.

Mr. LUNGREN. So that we have to take the entire law into effect with the amendments we have placed here, and you still have that category of electronic surveillance for which you do have to get a warrant, correct?

Mr. MCCONNELL. That is correct. Yes, sir.

Mr. LUNGREN. And nothing in this act changes that, as far as you are concerned, in the operation of the law.

Mr. MCCONNELL. That is correct. Yes, sir.

Mr. LUNGREN. Thank you very much.

Mr. CONYERS. Thank you.

The Chairman of the Constitution Committee, Jerry Nadler.

Mr. NADLER. Thank you.

Director McConnell, in a number of interviews that you have given as well as in speaking to us, you have said that it takes about 200 hours, that the objection to getting a FISA warrant is that it takes about 200 hours, to do each FISA court application for each phone number, is that correct?

Mr. MCCONNELL. Yes, sir. At a summary level, that is correct.

Mr. NADLER. Thank you. In the letter that Chairman Conyers, Mr. Scott and I sent you on September 11, we pointed out that if this is true, this would mean that more than 436,000 hours were spent on FISA applications in 2006, and you were asked specifically whether you still stand by that 200 hours assertion.

Your response, which we received this morning, frankly evaded that question and simply asserted that your point was that significant resources shouldn't be devoted to FISA applications.

So I ask you now, do you stand by the claim that it takes 200 hours to do each——

Mr. MCCONNELL. I do, and it is because of the complex nature of the process. First an analyst has to——

Mr. NADLER. All right. So you stand by that.

Mr. MCCONNELL [continuing]. To write it, and then so on.

Mr. NADLER. Now, and this morning in the Intelligence Committee, about 2 hours ago, the former or current director of the

FISA program, a Mr. Baker, testified that there is a—that basically his—that potentially contradicted that.

Essentially, what he said—and I am getting this secondhand from a Member of the Committee. Essentially, what he said—the record will show exactly what he said, obviously.

But essentially, what he said was that the legal preparation of the warrants is ready and waiting by the time the information that has to be gathered to figure out. That, in effect, within the executive branch the process is followed to put together much of the same information given to the FISA court in order to determine to begin surveillance, even where no warrant is sought. And that the work to get the warrant is not much extra work, and that they are usually ready at the same time.

Mr. MCCONNELL. On occasion, that is true, but sometimes it is not, often times it is not true, particularly if it is new——

Mr. NADLER. He said it was normally true. He said it was almost, in fact, usually true.

So if that is usually true, then how could it require the 200 hours? Because what he was saying is that most of the work that has to be done has to be done whether you need a warrant or not, just to identify it.

Mr. MCCONNELL. And, I am sorry, what is the question, sir?

Mr. NADLER. The question is if it is the case, as he apparently testified this morning, that most of the work that you say goes into this 200 hours for the warrant has to be done whether you need a warrant or not just to identify what you want to wiretap, to identify the target, and that the work required for the warrant is simply a little extra, then how can it be—then it is clearly not—I mean, what he said, essentially, was it is much extra work than what has to be done in any event.

Mr. MCCONNELL. Well, I just disagree with him. Having done it, having been the director of NSA and worked the problem, some of what he said is true, but when I say 200 man hours, I am talking about the entire process.

Mr. NADLER. But the entire process has to be done with or without the warrant requirement.

Mr. MCCONNELL. No, no. No.

Mr. NADLER. Or, excuse me, most of that has to be done with or without——

Mr. MCCONNELL. No, not at all.

Mr. NADLER. Well, that was his testimony this morning, and he headed the program.

Mr. MCCONNELL. I was the director of NSA, not him, so I could tell you that from the standpoint of conducting the operation, when you are doing foreign surveillance—remember, in the foreign context, and you have new information to process or to chase or target, it is just a matter of doing it in that—when it is in a foreign context.

So now if you have to stop and consider a warrant and so on, it presents you with a pretty formidable process to work through.

Now, Ben Powell, who is sitting to my right, just recently looked at this. Let me ask him to comment on his most recent review.

Mr. POWELL. I would disagree that there is any comparison to what we go through to target foreign intelligence targets and what we go through to put information together for the FISA court.

When we are targeting foreign intelligence targets, the analysts have to determine that there is a valid foreign intelligence target and a requirement is out there for putting that person on coverage.

To go through the FISA process is frequently a very long-term process that requires putting together packages that frequently resemble finished intelligence product, describing who the person is, what their organization is——

Mr. NADLER. So the essence of your testimony is contrary to what we heard in—and I wasn't there—what was heard this morning in the Intel Committee, that there is substantial extra work beyond what would be done if you don't need a warrant.

Mr. POWELL. If that is the correct testimony. I will say that Mr. Baker is very knowledgeable in this area, so I feel like we are missing something extra he must have said, because he is certainly very knowledgeable in this area.

Mr. NADLER. As I said, I got this from a Member of the Committee. I wasn't there. I presume that that was correct.

Let me ask you this. You said basically that the danger that we are talking about in targeting foreign people—now, again, everybody agrees that foreign to foreign should not be covered, rather, by FISA.

Everybody agrees to that. I don't want to talk about that. The question I want to ask——

Mr. MCCONNELL. No, but the term foreign to foreign is—that is what confuses——

Mr. NADLER. I understand. Foreign to foreign, whether the electrons come through the United States or not.

Mr. MCCONNELL. No, no, that is not the point. The point is if you have to predetermine it is foreign to foreign before you do it, it is impossible. That is the point. You can only target one.

Mr. NADLER. All right. I hear that.

Mr. MCCONNELL. The issue is who is the target and where are they.

Mr. NADLER. I hear that. The question I am trying to ask, though, is under FISA, under the FISA as it existed 3 months ago, my understanding is if you determined that somebody abroad—did you need a warrant to determine if someone abroad was, in fact, an agent of a foreign power, or could you make that determination for yourself, if he was communicating into the United States?

Mr. MCCONNELL. You could make the determination, but let me just make it very specific. If Osama bin Laden in Pakistan calls somebody in Singapore, and it passed through the United States, I had to have a warrant.

Mr. NADLER. Yes, but no one objects to changing that. My question was if someone in Pakistan calls someone in the United States, you want a warrant to target the guy in Pakistan. Did you need——

Mr. MCCONNELL. No, I don't want a warrant to target the guy in Pakistan.

Mr. NADLER. No, no, did you need a warrant under traditional FISA?

Mr. MCCONNELL. Under traditional FISA, if—no, I did not.

Mr. NADLER. You did not.

I see my time has expired. Thank you.

Mr. CONYERS. Thank you.

The Chair recognizes Howard Coble, the distinguished gentleman from North Carolina, Ranking Member of the Court Committee.

Mr. COBLE. Thank you, Mr. Chairman.

Good to have you gentleman with us today.

Admiral, as we all know, FISA was enacted in 1978. From that date of enactment, did FISA allow the intelligence community to intercept a phone call from a foreign target to a person inside the United States without a court order?

Mr. MCCONNELL. Sir, that is one of those questions. It depends. There are some conditions. Who is the target? Where is the target? And here was the key: Where is it intercepted?

And what we found ourselves in with old FISA is the issue was where it was intercepted. If it was here on a wire, then that is what put us in a condition where we had to get a warrant, where we did not back in 1978.

Mr. COBLE. Okay. Thank you, sir.

Now, Mr. Lungren may have touched on this, but for my information, distinguish, Admiral, between targeting an individual for surveillance and intercepting a phone call to or from an individual.

Mr. MCCONNELL. If you are going to target, you have to program some equipment to say I am going to look at number 1-2-3. So targeting in this sense is you are targeting a phone number that is foreign.

So that is the target. The point is you have no control over who that target might call or who might call that target.

Mr. COBLE. Mr. Wainstein, as the Admiral pointed out, this is a complex matter we are dealing with today. There seems to be a great deal of confusion about the application of FISA to domestic surveillance of United States persons.

Provide us with a simplified explanation, if you will, of when a FISA court order is required for United States persons.

Mr. WAINSTEIN. Congressman, I think as one of your colleagues said earlier, if we direct surveillance, we target somebody inside the United States, we have to get a court order from the FISA court.

If we surveille communications where both ends of the communication are within the United States, we have to get a FISA court order.

So that has not changed. Those aspects of the definition of electronic surveillance, or those requirements of the original FISA, are still in place, even with the Protect America Act. That hasn't changed that at all.

Mr. COBLE. I thank you, sir.

Mr. Chairman, I yield the balance of my time to the gentleman from California, Mr. Lungren.

Mr. LUNGREN. I thank the gentleman for yielding.

There has been some question about whether or not—and following up a little bit on what the gentleman just said, that somehow this is going to allow warrantless—can we interrupt?

[Audience outburst.]

Mr. CONYERS. You were saying, Congressman Lungren?

Mr. LUNGREN. I was saying I guess I don't have to go to Disneyland this year.

There has been some suggestion that under the terms—Mr. Wainstein, there have been some suggestion that under the terms of the Protect America Act this would allow unwarranted physical searches of homes or effects of Americans without a court order.

Can you respond to that particularly, please?

Mr. WAINSTEIN. Yes, sir. Thank you for the question. The question has been raised whether the statute as it is phrased, the Protect America Act, would allow us to take this authority that was clearly directed at our ability to get the assistance of communication providers, or telecommunications, and actually get assistance from a mailman to give us—you know, allow us to search mail, or somebody—a landlord to allow us to search a tenant's effects.

That is not the case, and I could go through—sort of parse through the statute, but the bottom line is there are various requirements that this—the Director of National Intelligence and the A.G. have to certify to that are satisfied here.

One of them is that we get the support, the assistance, of a communications provider. A communications provider is not going to be the one who is going to let us into a basement, not going to be the one who is going to let us see someone's mail.

So when you actually tease it out in the statute, these concerns, these sort of hypothetical scenarios, really don't play out.

In fact, this is something that we detailed in the letter that I sent to this Committee, I think, just earlier——

Mr. LUNGREN. Well, isn't it true that section 105(b) still specifically is a mechanism for the Government to obtain third-party assistance in the acquisition of communications of persons located outside the United States? Is that still a predicate?

Mr. WAINSTEIN. Absolutely. And it has to concern persons outside of the United States. And it also has to require that we get the assistance of a communications provider.

And also, I would like to make another point. Some people are concerned that we would nonetheless use it this way. Keep in mind that we are—as I said in my earlier statement, we are providing tremendous access to Congress to oversee this program, so you will see what it is we are doing.

The FISA court is receiving the procedures by which we conduct this surveillance. If the procedures allow that, they will see that that doesn't fit with the law.

And in fact, a person who receives a directive which is inappropriate can challenge it under this law, can go to the FISA court and challenge the appropriateness of that directive.

So there are a number of ways which would prevent us, even if we had a mind to do so, from using this authority in an unintended way.

Mr. LUNGREN. Thank you very much.

And I thank the gentleman for yielding.

Mr. COBLE. I will reclaim and yield back, Mr. Chairman.

Mr. CONYERS. Thank you.

Crime Subcommittee Chairman, Bobby Scott, of Virginia?

Mr. SCOTT. Thank you.

Admiral, we have had some confusion on when something is classified and when it is not. Is there some process that delineates when something is classified and when it is not classified?

We have had testimony here of things that were classified, and then you would read it in the paper. Does it become declassified just because you said it, or is there some process to declassify?

Mr. MCCONNELL. No, there is a process, but it is ultimately a judgment call.

Mr. SCOTT. Well, if it is a judgment call—but I mean, do we know, when does it become declassified? Is that when you just decide on the spot to blurt it out to a reporter?

Mr. MCCONNELL. No, not at all.

Mr. SCOTT. Is there some process?

Mr. MCCONNELL. There is a process but, as I say, it is ultimately the responsibility of the President to decide——

Mr. SCOTT. But there is a process. Do we know when something was declassified, the moment of time it was declassified, and is there some record of that?

Mr. MCCONNELL. Not specifically that I am aware of. I am sure it can be recovered in some way if there is a specific concern or question.

Mr. SCOTT. You said that the old law prevented you from getting intelligence and mentioned specifically conversations between al-Qaida from overseas talking to people within the United States, and now it is legal to intercept those communications.

If it is legal now, why couldn't you have intercepted those conversations with a FISA warrant, a FISA warrant obtained before, or after the fact if you are in a hurry?

Mr. MCCONNELL. The issue becomes volume and ability to keep pace. We could have targeted communications of al-Qaida, except when it touches a wire in the United States. That was the technical issue——

Mr. SCOTT. Wait, wait. You could get a warrant to get that. You just couldn't do it without a warrant.

Mr. MCCONNELL. Yes, sir. But what you have just now said is now you are requiring us to have a warrant for a foreign target in a foreign country. So the issue is there are lots of targets, and so we couldn't keep up.

Mr. SCOTT. But you are not—so you would just say it is a paperwork problem, it is not a prohibition in the law.

Mr. MCCONNELL. No, it is a practical problem.

Mr. SCOTT. But you can get that information, you could get that information——

Mr. MCCONNELL. No, sir. I cannot. Think about foreign intelligence. I mean, there are thousands, potentially millions, of potential targets of interest, so the process just couldn't turn fast enough, if we were required to get a warrant for every one of those.

Mr. SCOTT. And if you felt you needed some information, even the after-the-fact warrant would not solve that problem?

Mr. MCCONNELL. Would not, no, sir.

Mr. WAINSTEIN. And if I could add, you would also, in that sense, be required—you would not just make the showing that it is a valid foreign intelligence target that we do in our foreign intelligence col-

lection. Under FISA, you would have to be making a probable cause showing concerning that foreign person overseas.

So it is not the case that in every situation where we had a valid foreign intelligence target we would make a probable cause showing to the FISA court. It is not the case that, in any sense, we could do that for every valid foreign intelligence target——

Mr. SCOTT. So anybody overseas, you don't have to make any ascertainment about who they are, any call into the United States you can listen to.

Mr. MCCONNELL. Foreign, yes, sir, if it is a legitimate foreign intelligence target. I mean, there are practical limitations.

Mr. SCOTT. Well, wait a minute. Wait a minute. You just said you didn't, it is not a target. It is just somebody.

Mr. MCCONNELL. Well, let's insert some practicality here.

Mr. SCOTT. If you practically target somebody as a terrorist overseas, there is no problem, there is no legal impediment to you getting a warrant to who they are calling.

Mr. MCCONNELL. Now, under the new act, that is correct. Under the old act it was.

Mr. SCOTT. No, under the old act you could get a warrant.

Mr. MCCONNELL. I could get a warrant, that is correct.

Mr. SCOTT. Okay.

Mr. MCCONNELL. The issue was I was required to get a warrant.

Mr. SCOTT. Okay. You would just save a little more paperwork. Okay.

Mr. MCCONNELL. Well, I wouldn't characterize it as a little more paperwork.

Mr. SCOTT. The section 105(b) authorizes you to get foreign intelligence information "concerning"—now, the word in the section 105(a) is "directed at a person." In 105(b) it is "concerning persons believed to be outside the United States."

That is a different word, and why wouldn't we conclude that you are supposed to have a different meaning, that the subject matter of the conversation is concerning a person to be outside of the United States?

Mr. MCCONNELL. Sir, that is complex. I want to ask counsel to respond. There are reasons for the choice of words. From my perspective, we want to be effective, so if there is a better word, I would be happy to consider it.

But let me ask counsel to respond to your specific question.

Mr. POWELL. In terms of the actual drafting, sort of whose idea it was, and actually what rationale there was for putting that in there—I can't speak to that myself, but I think that when you look at it, you realize that given the circumstances under which this was actually drafted, it was intended to allow us to fill an intelligence gap.

Mr. SCOTT. Well, let me just—I am running out of time. Acquisition of foreign intelligence information concerning persons reasonably believed to be outside of the United States—now, the gentleman from California went to great lengths to say you have to have it in context with all these other laws.

Unfortunately, section 105(b) starts out with the phrase "notwithstanding any other law." Now you say you are authorized in

the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States.

Now, why couldn't we conclude somebody calling—two people in the United States talking to each other about Tony Blair—concerning a person—he is believed to be outside the United States. Why shouldn't we conclude that you are trying to get into that conversation without a warrant?

Mr. WAINSTEIN. Well, that is the point that Congressman Lungren made, which is that the rest of FISA, the rest of the definition of FISA——

Mr. SCOTT. Well, no. "Notwithstanding any other law" starts off that section, which cancels out all that.

Mr. LUNGREN. Will the gentleman yield on that point? Will the gentleman yield on that point?

Mr. SCOTT. I will yield.

Mr. LUNGREN. If it said "notwithstanding any other section of this law" I think your point would be valid. It says "notwithstanding any other law," provision of law. It still is within the context of FISA.

Mr. SCOTT. Well, notwithstanding any other law—authorize acquisition of foreign intelligence information concerning—now, these words mean something, and you pointed out that there are—you intentionally chose different words not directed at a person reasonably believed to be located outside the United States.

It is concerning persons reasonably believed to be outside the United States. Now, would that include, say, a conversation? Suppose you have a war protester in Iraq calling a war protester in the United States. That is foreign intelligence, isn't it? Is that foreign intelligence?

Mr. POWELL. We are prohibited from doing anything solely on the basis of activities prohibited by the first amendment. That is a bedrock principle of the intelligence community operations. A war protester——

Mr. SCOTT. Where is that in here? Where is that in here?

Mr. POWELL. That has been a bedrock principle of the intelligence community. That is in Executive Order 12333. That is in the National Security Act. That is a bedrock principle that is part of every person's training in the intelligence community.

A war protester exercising their first amendment rights is not a valid foreign intelligence target.

And if I may answer the other hypothetical involving the notwithstanding any other law, if you read the conditions under which certifications may be made within that section, we have to certify that the acquisition does not constitute electronic surveillance.

Electronic surveillance, as defined in the act, remains the same. If the sender and intended recipient are both within the United States, we are required to get a court order. That would remain electronic surveillance.

That is the specific reason why, in this provision, it says that they can only certify it when it says the acquisition does not constitute electronic surveillance.

Mr. SCOTT. Does that include e-mails? Does that include e-mails?

Mr. POWELL. The acquisition does not—I don't think that—it is communications, foreign intelligence information. It cannot con-

stitute electronic surveillance. So if it is a domestic communication captured, it would be included.

Mr. SCOTT. Is an e-mail included in the exclusion? Can you get an e-mail, domestic to domestic, talking about someone outside of the United States?

Mr. POWELL. I believe that would constitute electronic surveillance——

Mr. WAINSTEIN. It would require a warrant.

Mr. POWELL [continuing]. And require a court order.

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

Mr. WAINSTEIN. May I just add one thing, Mr. Chairman, just to follow on to your question about the exercise of first amendment rights?

In FISA, actually, section 1805, it says the targeted electronic surveillance—we have to show the targeted electronic surveillance the foreign power—provided that no U.S. person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment of the Constitution of the United States.

Mr. SCOTT. Wait a minute. You don't have to be a foreign power, because you just have to be outside of the United States.

Mr. WAINSTEIN. Yes. You were asking about where that provision is. That is actually in the original FISA when it talks about our showing of somebody being a foreign power——

Mr. SCOTT. Well, you are not getting a warrant under FISA. You are just designating somebody out of the country calling in. And the question is whether you can pick up some foreign intelligence.

Mr. WAINSTEIN. Yes. Well, and that goes to what Mr. Powell said about the guidance and the various policies of the intelligence community. I was saying that that has actually been codified in FISA as well, and I think it is something that permeates all our activities.

Mr. CONYERS. In other words, it could be clearer.

The Chair recognizes Steve King, Ranking Member of Immigration, from Iowa.

Mr. KING. Thank you, Mr. Chairman.

And I thank the witnesses.

I have to back up a little bit, and I would like to——

[Audience outburst.]

Mr. Chairman, I would ask if you might just simply reset my clock. I don't know if it actually got set and seems to be blank up there.

But I would ask Director McConnell if you could take us back to this decision by the FISA court that it required a warrant, foreign to foreign, if the conduit happened to be within the United States.

And as I read through some of the documents on that, I didn't recognize the name of a judge or the names of a panel of judges that had made that decision. Have we identified the brain or the brain trust that came to such a conclusion? And is that something that is unclassified?

Mr. MCCONNELL. Sir, it wasn't a judge. It was an interpretation of the statute. And there are 11 judges on the court, and as you know, judges are independent and they exercise their own reading of the law, their interpretation of the law.

So in the case of the FISA review, we have to get an update every 90 days. So when we subjected the request to the FISA court, the first review kept us where we needed to be with regard to the targets we need to collect and so on.

As the subsequent review continued after the 90-day renewal period, subsequent judges started to define it a little more narrowly.

So what we found is we were actually going backwards in our ability to conduct our surveillance, which was requiring a warrant for a foreign target in a foreign country. And the issue was the wording of the law from 1978. If it touched a wire in the United States, we had to have a warrant. That was the basic issue.

Mr. KING. Well, and I thank you for that clarification, but it was incremental changing, apparently, of a realization or an analysis that took place, as you saw that 90-day report come out.

And I wanted to also ask you, was our national security put at risk because of that decision?

Mr. MCCONNELL. Oh, yes, sir. Definitely. We were in a situation where we couldn't do our basic function of provide warning or alert to stop an attack.

Mr. KING. And for how long, Director?

Mr. MCCONNELL. We had a stay until the end of May, and we weren't able to go back up on full coverage until the new law was passed on the 5th of August.

Mr. KING. Okay. So we had June, July, about 8 weeks to 9 weeks there all together, that the national security of the United States was jeopardized because of what—and I am not taking issue with the analysis of the language that was there, because I recognize that it was written in 1978, and we had this transition that took place.

But I wanted to ask you about your understanding of your oath to the Constitution——

Mr. MCCONNELL. Yes, sir.

Mr. KING [continuing]. And to the rule of law, and some of these come down to some very difficult questions. I know internally I have been conflicted a number of times myself.

But if it meant saving the lives of Americans and recognizing a judicial opinion that has been kind of a moving opinion, really when it came down to that real decision, if it came down to black and white, and not having alternatives—and we had a 9-week window here—where does your priority fall on your oath and your understanding of that oath compared to our national security?

Mr. MCCONNELL. Well, my first responsibility is defend the Constitution and protect the country, so that would be a very, very hard choice.

My preference, and the reason I have gone further than any other senior official in this community to talk openly about it, is to get us in the right place with the right kind of debate in the Congress and understanding by the public.

So that is a very difficult question. In the final analysis, I would protect the country.

Mr. KING. And yet we had about a 9-week window there when we weren't—I mean, if we suspended surveillance under those conditions during that period of time——

Mr. MCCONNELL. Yes, sir.

Mr. KING [continuing]. If you weren't doing anything then, that would be the only scenario by which the United States didn't become more vulnerable during that period of time.

Mr. MCCONNELL. Right. What we did do was, as the numbers got smaller, we prioritized in a way that we kept the most important, the most threatening, on coverage.

And we worked very quickly to try to catch up, and what we found is the—there is so much volume that we were falling further and further behind. That is why we made it such a critical issue to try to get the attention and focus on it in July.

Mr. KING. And yet when we did finally pass the update law on August 5—and it was signed into law same day, I think, as final passage, if I recall correctly—the President understood the urgency.

Mr. MCCONNELL. Yes, sir. The 4th it was passed. It was signed the next morning on Sunday, the 5th.

Mr. KING. Okay. And then did it take some time to get ramped back up again, to get back up to speed?

Mr. MCCONNELL. It actually took us about 5 days to get it all done, because there were new procedures, and we had to be very careful, so we had the highest priority on coverage, and then it took us about 5 days or so get back to where we were in January of this year.

Mr. KING. So what happens to national security if some of the amendments to this law that have been discussed here today are applied?

I mean, you have testified to that a number of times, but 200 hours per warrant—what percentage of your effectiveness might be diminished if this law is amended in the fashion that is advocated?

Mr. MCCONNELL. If we go back to the original interpretation and the way it was being interpreted by the FISA court, we would lose about two-thirds of our capability and we would be losing steadily over time.

Mr. KING. Thank you, Director. I appreciate your service to America and your testimony today.

And yours as well, Deputy.

And I would yield back the balance of my time.

Mr. CONYERS. Thank you.

Chairman Howard Berman, Courts Subcommittee, California?

Mr. BERMAN. Thank you, Mr. Chairman.

I just might say parenthetically that I am unaware of anyone who is suggesting we just go back. There are differences, but I think that is a straw man, that hypothetical.

I have a few questions, but first I would like to yield a minute to my colleague from California to follow up on some earlier comments made in the Chairman's questioning.

Mr. SCHIFF. I thank the gentleman for yielding, and I will be very quick.

Mr. Director, I just want to follow up on the Chairman's questions at the outset.

I don't think the Chairman was asking how often you have attempted to get a warrant on an American, which I think you have stated that you have done about 100 times, but rather where you have gone up on a foreign target but have had the effect of over-

hearing the conversation of an American. How often has that happened?

And I think you said you would get the number back to us, but I wonder if you can tell us today, are we talking about hundreds of conversations, thousands of conversations, or tens of thousands of conversations?

Mr. MCCONNELL. Sir, I simply don't know. I mean, I just don't know. We will get the number and provide it.

Mr. SCHIFF. I would think as the Director you ought to know what ball park we are talking about even if you don't know the specific number.

Do you have any objection to——

Mr. MCCONNELL. I am not even sure we keep information in that form. It would probably take us some time to get the answer. The reason is you are collecting information. It is in a file. It will roll off in a period of time.

You may not even know it is in the database. That is one of the reasons we are so careful about who has access to that database.

Mr. SCHIFF. If I could just—because I don't want to take up too much of Mr. Berman's time.

Do you have any objection, Mr. Director, to an amendment to the Protect America Act that would provide that when you do overhear the conversation of an American, even though you are targeting a foreigner, that you will report those conversations to the FISA court, that the FISA court would have a supervisory role as well as the Congress?

Since that would be done on the back end, it wouldn't provide any time obstacle or anything to the surveillance on the front end. Would you have any objection to that kind of an amendment?

Mr. MCCONNELL. Sir, all I would say is when you—what I was trying to get out earlier—when you are collecting information, think of it as a broad area targeting foreign communications.

More often than not, you don't even know that communication is in the database, so it might—and I don't know; I would be happy to take a look at it. It might create a situation where it creates significantly extra effort on our part—don't know, but happy to take a look at it.

Mr. BERMAN. Just reclaiming my time, how do you know, if you are minimizing those conversations, how come you wouldn't know? How do you minimize without knowing?

Mr. MCCONNELL. If you look at it, then you know.

Mr. BERMAN. So all you do is minimize the ones you happen to look at.

Mr. MCCONNELL. Right. If there is something in there that—it doesn't come up for some reason, you just wouldn't know. That is what I was trying to make the Committee sensitive to.

Mr. BERMAN. Mr. Wainstein, it seems to me there is a fruitful area, based on your letter, to proceed in. I want to make sure I understand.

You state that the bill we passed does not give you the authority for physical searches of homes, mail, computers or personal effects of individuals in the U.S., and you won't use it for such purposes.

There are people who are concerned about that. As part of being able to do what you need to do, would you have any objection to—

as part of a permanent or subsequent authorization, prohibiting—making clear that that is not authorized?

Is there any problem with that, that which you have asserted without qualification is not allowed?

Mr. WAINSTEIN. Right. I have been asked that question a number of times—well, that is not a problem. If you don't read the statute to allow that, then why not go ahead and put some sort of proviso in the statute that says that it is not allowed, and that is—as I said, we are perfectly happy to see any proposed language you might have.

You have got to keep in mind, though——

Mr. BERMAN. Maybe we will just take it from your letter.

Mr. WAINSTEIN. Keep in mind, however, sir, that, you know, every time you put language in—see, here you are talking about authorizing language that some people think might has unintended consequences.

If you put limiting language in, you have got to make sure that that doesn't have unintended limiting consequences. So it has to be looked at very carefully. But I would be happy to look at it.

Mr. BERMAN. But you are open to that avenue of pursuit.

You state collection of business records of individuals in the United States because they concern persons out of the United States. We want to make clear we will not use this provision to do so.

I guess I have the same question. You don't think this provision authorizes collection of medical or library records for foreign intelligence purposes.

Mr. WAINSTEIN. Well, there is no hesitation there. You know, my reading of the statute is it does not permit that.

Mr. BERMAN. And then I have same question regarding a bill that would make people feel more comfortable about this and at the same time not alter what you think the bill that passed in August does.

Mr. WAINSTEIN. We would be happy to take a look at the language, sir, yes.

Mr. BERMAN. And third, the issue of reverse targeting. I notice here you say the Government cannot, in other places you say the Government will not, do it.

Here you say the Government cannot and will not use this authority to engage in reverse targeting, the targeting of a U.S. person by the—your interest is in the U.S. person but you talk to the foreign person, because the U.S. person you think will be communicating with him.

Is there some subtle reason, or did you just decide to use a new formula when you added "cannot" to "will not" use that——

Mr. WAINSTEIN. That might have just been a little rhetorical flourish. I am not sure. Maybe I just wrote that late at night.

But I think the point was very clear. We cannot under the statute. That is not allowed. When we direct surveillance at somebody in the United States under FISA, under the preexisting definitions of FISA, we cannot do that without a court order, and we will not do it.

Mr. BERMAN. So it would just seem to me, as part of giving you the ability to do what you need to do, and having the American

public or that part of the American public and the Members of Congress that are concerned about other authorities, a fruitful avenue to pursue jointly would be to clear the underbrush out.

Those things that you don't think you are authorized to do and aren't seeking authorization to do, we specifically and affirmatively indicate clearly you can't do.

Mr. WAINSTEIN. Perfectly happy to engage with you on that process, and I guess I would just say——

Mr. BERMAN. A healing process.

Mr. WAINSTEIN [continuing]. In the context, though, of the recognition that there is ample congressional oversight, there is FISA court oversight, and you have got a commitment that we are not going to do anything, and that it would be against the law to do the reverse targeting as you just described, so——

Mr. BERMAN. I don't feel overwhelmed with the ampleness of the congressional oversight at this particular moment, but——

Mr. LUNGREN. You are part of it.

Mr. WAINSTEIN. We will be briefing you at any time you ask.

Mr. BERMAN. I reassert my position.

[Laughter.]

Mr. MCCONNELL. Sir, we feel overwhelmed right now with the number of visits we have had since the 5th of August. But could I just comment, if I would, where we got tension in the system last time is people were adding words and we didn't have a chance to examine them, so this unintended consequence thing is very important. As sort of the——

Mr. BERMAN. I appreciate that, and that is an argument for what I am suggesting as well——

Mr. MCCONNELL. Right.

Mr. BERMAN [continuing]. Because there are other people who fear consequences.

Mr. MCCONNELL. The other way.

Mr. BERMAN. They won't even assume that they were unintended. They think they may have been intended consequences, but you are up here telling us in writing and in person they were never intended, and we want to dispel that concern on that side.

Mr. MCCONNELL. And my point is if we can sit down and walk it all the way through, examine each word and understand it and accept it, then that is perfectly acceptable to the Administration.

Mr. BERMAN. Very good.

Thank you, Mr. Chairman.

Mr. CONYERS. That is a fine idea. That is what we ought to have been doing all the time.

The Chair recognizes the distinguished gentleman from Florida, Mr. Feeney.

Mr. FEENEY. Thank you, Mr. Chairman.

Admiral McConnell, thank you for coming today. The purpose of the hearing, as I understand it, is to review the recent changes enacted by Congress over the summer and the proposal to extend those.

I want to make sure I have this in context, because those changes were very limited, as I understand them. And so from a historical perspective—and you are very familiar with this from your time at the NSA.

In 1978, in the aftermath of concerns about some domestic surveillance activities and presidential powers, Congress, led by a Democratic majority, enacted FISA. Is that right?

Mr. MCCONNELL. Yes, sir.

Mr. FEENEY. And nothing in FISA precluded any surveillance activity between a foreign target and another foreign target.

Mr. MCCONNELL. That is correct.

Mr. FEENEY. And all of this was before 9/11, before we had been attacked on our soil actually with any serious success since the War of 1812; at least the continental U.S., putting aside Pearl Harbor.

And so presumably the intelligence community would have at least as much interest in foreign surveillance after the 9/11 attacks as it had before the 9/11 attacks.

Mr. MCCONNELL. Yes, sir.

Mr. FEENEY. And in the meantime, after the enactment of FISA, we have had this complete reversal in terms of the way the majority of communications take place.

It used to be that with respect to international communications, most of them were done in a wireless——

Mr. MCCONNELL. That is correct.

Mr. FEENEY [continuing]. Method, while domestic conversations typically took place over the wires.

Mr. MCCONNELL. Yes, sir.

Mr. FEENEY. And now we have had a reversal, where most domestic conversations take place wirelessly, but the majority or the preponderance of the international conversations actually take place on hard line.

Mr. MCCONNELL. Yes, sir.

Mr. FEENEY. And many of those hard lines, if not a majority, go through the United States at some point.

Mr. MCCONNELL. That is correct.

Mr. FEENEY. And so that under FISA, in order to give its original intent meaning, under now obsolete technology, all we really did was to modernize the ability of our intelligence people to look at a foreign target communicating with somebody else.

Mr. MCCONNELL. Yes, sir. That is correct.

Mr. FEENEY. And there is concern about whether or not the people that receive the communication from the foreign target that may be located in the United States, whether there are tens of them or hundreds or thousands—and you don't even know whether you keep records according to those lines.

But before the changes took place this summer, if a foreign target had used the old international technology to correspond with somebody in the United States, was there any specific protections for the individual American that received correspondence from a——

Mr. MCCONNELL. No, sir, it would not require a warrant, and then if it did involve an American, we would go through a minimization procedure.

Mr. FEENEY. In order to go forward, which you are still doing today.

Mr. MCCONNELL. Yes, sir.

Mr. FEENEY. And in fact, now you are required, which you were not required before these acts—if an American has received a communication from a foreign target, you are now required to minimize, which was not true before these new enactments.

Mr. MCCONNELL. Actually, it was true even in the old days.

Mr. FEENEY. It was true in the old days.

Mr. MCCONNELL. Yes, sir. Minimization has been consistent since 1978.

Mr. FEENEY. But the point is that American citizens have not lost—other than the fact that the technology has changed and we are after the same substance of communications, American citizens haven't lost any substantive or procedural due process rights or rights under the bill of rights.

Mr. MCCONNELL. That is correct.

Mr. FEENEY. Okay. I wanted to make that clear, because the whole purpose of these hearings seems to be the notion that we have empowered under the guise of foreign intelligence all sorts of snooping on Americans, and that is just not my understanding from the facts.

It seems to be totally disassociated with reality. And I think a lot of us are concerned with civil liberties. But we ought to get our facts straight before we go through that.

The other major change that the President is asking for, Mr. Wainstein, is with respect to immunizing communications companies and others that cooperate. Why is that important?

We have just established that citizens haven't lost any rights, despite the hullabaloo. Now why is it important to make this additional change?

Mr. WAINSTEIN. Well, I think it is a—I mean, a couple points. One, I think it is sort of fundamentally unfair and just not right to—if a company allegedly assisted the Government in its national security efforts, in an effort to defend the country at a time of peril—that they then get turned around and face tremendously costly litigation and maybe even crushing liability for having helped the United States government at a time of need.

So I think it is sort of just a general fairness matter. It is just not right.

Secondly, keep in mind that every time we have one of these lawsuits, very sensitive information gets discussed and gets leaked out or, you know, disseminated out in the public, and our adversaries are smart.

Both the terrorists who might be over in, you know, some place in the Middle East are smart, and then the governments that might be our adversaries are tremendously sophisticated, and they are gleaning all this information that gets out, and that is a tremendously, you know, concerning thing.

Also, just in terms of the disclosure of information about the fact that a company might have cooperated with us in national security efforts might well put that company's asset that happened to be overseas in some jeopardy. That is a very real concern for these companies.

So I guess those are three of the reasons why I think that is a very important part of the bill that the DNI submitted back in April of this year.

Mr. FEENEY. I yield back, Mr. Chairman.

Mr. CONYERS. Thank you, sir.

The Chair recognizes the very patient Chair of Immigration, Zoe Lofgren, of California.

Ms. LOFGREN. Thank you, Mr. Chairman.

Mr. CONYERS. Excuse me.

Ms. LOFGREN. I thought Mr. Watt was going to go before——

Mr. CONYERS. He wasn't here the last time I looked, but I will withdraw that invitation and recognize the distinguished gentleman from North Carolina, Mel Watt.

Mr. WATT. Thank you, Mr. Chair. I thought I had been here pretty much the whole time.

But let me direct this question to all three of you so as not to have to individualize it.

Mr. King in his questions referred to, and in the answers, you referred to a 9-week window when there were questions about the legality of some aspects of what had been done.

Are any of the three of you aware of which telecommunications companies continued to allow surveillance during that time period?

Mr. POWELL. There was nobody who was—we were operating, and we have since January, under——

Mr. WATT. My question is are you aware of any companies that continued to allow surveillance. I am not trying to cut you off, but if the answer is no, then I think that would be the answer. If the answer is yes, then I would be happy to listen to your explanation.

Mr. POWELL. Anyone who was providing us assistance was doing so under FISA court orders. I am not aware of anyone providing assistance outside of valid FISA court orders during that window. We simply had a gap.

Mr. WATT. Any of you aware of any Administration officials who made promises to seek retroactive immunity as part of the FISA revisions to any telecommunications companies to get them to cooperate with the terrorist surveillance program or any other surveillance programs?

Mr. MCCONNELL. No promises, but that was included in the bill that we submitted back in April. That was a part of the——

Mr. WATT. I understand it was in the bill.

Mr. MCCONNELL. No promises.

Mr. WATT. I am asking you whether anybody in the Administration, to your knowledge——

Mr. MCCONNELL. To my knowledge, no.

Mr. WATT [continuing]. Made any promises that that would be part of what was being sought to gain their cooperation.

Mr. POWELL. There was no need to in the sense that we have always seen that as a very high priority to get that. It was always a high priority. It was in our bill, and it was something that the DNI has always emphasized in his statement, so I don't know——

Mr. WATT. Are any of the three of you aware of any assurances that any member of the Administration gave to any telecommunications companies that the Administration would seek to dismiss on national security grounds any lawsuits challenging the telecommunications companies' cooperation with any of the surveillance programs?

Mr. MCCONNELL. I am not aware of any promises like that.

Mr. POWELL. No, sir.

Mr. WATT. My question was addressed to all three of you.

Mr. POWELL. I don't know of any assurances. It certainly is the case that when intelligence activities are disclosed in an unauthorized manner—this was the case that we were going to seek to dismiss, to protect sources and methods.

So it is not a question of assurances or promises. I think everyone knew that was the course that this would be launched on.

Mr. WAINSTEIN. Yes, I think that has been quite clear from the initial disclosure of the——

Mr. WATT. And what specifically can you identify that the telecommunications companies did that is not already covered by the immunities under the FISA program?

What is it that we are putting this provision in the law to protect against, other than the generalized concern that Mr. Wainstein referred to?

Mr. WAINSTEIN. Well, FISA has its own immunity provision. The Protect America Act has an immunity provision.

Mr. WATT. That is the point I am making. What is it that we are seeking to hold them harmless against, other than what FISA already holds them harmless against?

Mr. WAINSTEIN. Well, as you know, a number of telecommunications companies have been sued around the country for a variety of different alleged types of assistance that they allegedly provided to the Government after 9/11 in the Government's surveillance efforts.

And so it would be that range of activities, and a number of them cite the program which has been described as the terrorist surveillance program.

Mr. WATT. And you are proposing that we write some language that would absolutely cut off the right to sue, or, is there some language that we are just going to retroactively immunize whatever actions were taken under the provision that you propose?

Mr. WAINSTEIN. Well, the Director of National Intelligence proposed—one of the provisions submitted in the FISA modernization proposal in April—one of them is retroactive immunity back to 9/11.

Mr. WATT. Let me ask the question again. What is it that we are immunizing them from, that you are seeking to immunize them from?

Mr. MCCONNELL. Alleged cooperation with the community to conduct foreign surveillance. Alleged cooperation with the intelligence community to conduct foreign intelligence.

Mr. WATT. How many lawsuits are already out there?

Mr. MCCONNELL. Sir, I don't know. I don't know.

Mr. WATT. And you don't think that is a relevant consideration?

Mr. MCCONNELL. The number?

Mr. WATT. Yes.

Mr. MCCONNELL. I am sure it is relevant. I just don't personally know. I haven't tracked it in that level of detail.

Mr. WAINSTEIN. Sir, I don't have the exact number, but I think it is somewhere in the range of 40 or 50 or so different lawsuits.

Mr. WATT. And have you all done an analysis of these lawsuits to determine whether any of them have any justification? That is

what you are seeking to have us immunize the Government from, right?

Mr. WAINSTEIN. Yes.

Mr. WATT. Or immunize the telecommunications companies from. Has anybody evaluated them individually to determine whether any of them have merit?

Mr. WAINSTEIN. I have not personally, but we have a civil division in the Department of Justice that has been working on these cases and they have gone through the merits of these cases. And they would have done that.

Mr. WATT. I yield back, Mr. Chairman. I appreciate it.

Mr. CONYERS. Thank you.

The Chair recognizes the Ranking Member of Constitution Subcommittee, Trent Franks, of Arizona.

Mr. FRANKS. Well, thank you, Mr. Chairman.

And thank you, gentlemen, for being here.

Admiral McConnell, I have heard you both in classified setting and in open setting, and I will just say to you that I am grateful that a man of your commitment to freedom, to the Constitution and clarity of mind is watching over my family. Very grateful to you, sir.

With that, there have been a lot of hypotheticals here, so tongue in cheek, what if we lived in a world where there were no hypotheticals, hypothetically speaking?

And the reason that I bring that up is because there is so many hypotheticals here that have been put forth that have so little to do with the real issues here, and I have been very impressed with your ability just to clarify things in ways that everyone can understand.

But let me just, if I could, even though it is redundant, is it not true that, say, in Florida that if Osama bin Laden was in a hotel and was making a call to someone outside the country that you could not tap his phone or surveille his phone without a FISA warrant? Is that not true?

Mr. MCCONNELL. Yes, sir, that is correct.

Mr. FRANKS. Even if you reasonably believed it was Osama bin Laden himself?

Mr. MCCONNELL. Yes, sir. It would require a court order.

Mr. FRANKS. So the bottom line is, to make it very clear, no one living inside the United States is being surveilled without a warrant.

Mr. MCCONNELL. That is correct, if they are the target of the surveillance.

Mr. FRANKS. If they are the target of the surveillance, yes, sir. No one is being targeted for surveillance in the United States without a warrant.

Isn't it also true that you have some familiarity with the Constitution itself and the fourth amendment?

Mr. MCCONNELL. Yes, sir.

Mr. FRANKS. And that you are committed under your own oath to uphold and defend that constitutional——

Mr. MCCONNELL. I am.

Mr. FRANKS [continuing]. Part of the Constitution? So if indeed there was some statute out there that we didn't quite write right,

hypothetically speaking, you would be bound both morally in your own mind and by the Constitution of the United States that that fourth amendment would transcend any failed statute.

Mr. MCCONNELL. Yes, sir.

Mr. FRANKS. Yes. You know, given the nature of the executive orders and the non-statutory guides that were kind of discerning parameters of intelligence-gathering activity, let me put it this way.

Sometimes the intelligence-gathering parameters are dictated in some detail by executive order as opposed to statute. Now, there are some here that believe that we need to have a statute for every one of those things.

But analyzing that from a separation of powers point of view, and from a practical standpoint, if the Congress put forth every detail in every situation as to what parameters you could use for foreign intelligence that would transcend any of the executive orders, what would be the implications of that?

Mr. MCCONNELL. Sir, it wouldn't be, we couldn't be, flexible enough to be responsive to an evolving situation, so currently the laws are broad, broader. And then Executive Order 12333 is actually how we execute the law and conduct our business, so it allows you more flexibility.

Mr. FRANKS. And the practical challenge of getting a FISA court order for every foreign surveillance target is overwhelming, is it not?

Mr. MCCONNELL. Yes, sir. In this case we are discussing, we were limited strictly to just al-Qaida, just al-Qaida, and we couldn't keep up. So if it is foreign intelligence broadly speaking, weapons of mass destruction, that sort of thing, it would be impossible, physically impossible.

Mr. FRANKS. Mr. Chairman, I have one last premise and then a question for the entire panel.

Given the kinds of enemy that we face in today's world, intelligence and knowing what they are going to do, given the fact that there is very little way to deter their intent, we have to ascertain their plan and capacity.

Given the nature of the enemy that we face today, it should stand obvious to all of us that intelligence is by far the most important aspect of this battle. If we knew where every terrorist was today and what their plans were, we could end terrorism within 60 days.

So with that in mind, do you think that some of the bills that are being postulated here that would potentially preclude you from being able to surveille foreign intelligence targets, how serious a threat do you think that is to our national security?

Mr. MCCONNELL. Sir, the majority of what we know about these terrorists comes from this process, so my greatest concern is that in passing a bill where you don't fully understand all the unintended consequences, it could literally shut us down, as it did when the technology changed from 1978 to currently. The interpretation of the law literally shut us down.

Mr. FRANKS. Yes.

Well, thank you all very much.

And thank you, Mr. Chairman.

Mr. CONYERS. The very patient Chair of Immigration, Zoe Lofgren, California?

Ms. LOFGREN. Thank you, Mr. Chairman.

In a recent article in the Washington Post, a scientist at Sun Microsystems, Susan Landau, expressed concern that the new technologies that are being used in the broadening intelligence-gathering efforts themselves create a national security vulnerability and, to oversimplify her thesis, would actually provide a portal into the telecommunications stream that could be exploited by our enemies.

The systems being used domestically I assume are likely to be the ones fielded abroad, but they will be U.S.-based. So here is my question.

Regarding NSA surveillance systems abroad, has anyone other than the United States government ever been able to use those systems to their advantage?

Mr. MCCONNELL. You mean the tools and techniques we would use abroad? Is that the question?

Ms. LOFGREN. The systems that we have deployed abroad to accomplish this surveillance—have those systems ever been used by others to their advantage?

Mr. MCCONNELL. Well, we have allies with which we share a lot of our collective effort.

Ms. LOFGREN. Well, the question is not with our permission, but adversely.

Mr. MCCONNELL. Others, other countries using similar techniques?

Ms. LOFGREN. Or an enemy of ours. Has anyone been able to use those?

Mr. MCCONNELL. Yes. Yes, there is evidence of other countries attempting to use similar collection techniques.

Ms. LOFGREN. Has there been successful use by others of those systems to their advantage?

Mr. MCCONNELL. Let me answer it to not say successful use of those systems, because I am not sure what you are referring to, but are others using electronic surveillance against the United States and its allies—the answer is yes.

Ms. LOFGREN. Perhaps we can explore this further. I know we are going to have a closed session, and perhaps we can explore this issue further in that venue.

Mr. MCCONNELL. Be happy to, ma'am.

Ms. LOFGREN. I want to get back to the immunity issue. If no one has done anything illegal, it is not clear to me why we need to immunize past behavior.

And it seems to me that at a minimum, if we are going to do that, we ought to know specifically what the behavior is that we are immunizing.

Are you prepared to let us know about that behavior either here or in a another setting?

For example, we understand that there was a period in March of 2004 where the Administration proceeded in wiretapping without even an attorney general's authorization because both the attorney general and then acting attorney general, Jim Comey, refused to certify the program.

Are there other periods that we are going to be immunizing and other programs that we are going to be immunizing?

Mr. MCCONNELL. To answer your first question, would we be willing to share what we are discussing, yes, we would, in closed session.

With regard to your question about 2004, I personally can't answer it because I wasn't in the Government, or I don't have any personal awareness, but maybe my colleagues know.

Ms. LOFGREN. If you are suggesting that this would be better reported to us in closed session, that is an acceptable answer to me.

Mr. MCCONNELL. Yes.

Ms. LOFGREN. I don't want to do anything that would jeopardize our Nation's security.

I have a question, really, about what started this issue, and it is something that troubles me a great deal.

It has been referenced publicly that there was a decision by the FISA court that reached the conclusion that you could not obtain information that was from a foreign source, from a person abroad to a person abroad, that was merely routed through the United States.

And I think there is 100 percent agreement in the Congress that that is something that we would want to remedy. I don't think there is a fight about that.

But we have never seen the decision. And I think we should see the decision. And I wonder whether the decision was appealed. And you know, if it needs to be done in a confidential setting, I think that is fine.

But to some extent, we are being asked to buy a pig in a poke here, and I don't really think that is the role of the United States Congress.

Mr. WAINSTEIN. No, thanks for the question, Congresswoman. I think we have got to be careful about sort of putting too much of this on any particular FISA court decision.

The problem, as has been identified by a number of Members here, is with the original statute, and then with the evolution of technology since the original statute was drafted.

And somebody has articulated it quite well earlier. You know, the problem is that you often—while you know where communications come from——

Ms. LOFGREN. So the information we got earlier about this decision was not correct?

Mr. WAINSTEIN. I am not exactly sure what information you got, and I am always reluctant to talk about what did or didn't happen in the FISA court because, you know, much of that is very sensitive.

But I guess if I may, for purposes of this debate, it is the statute itself that is the issue, and that is the problem, so——

Ms. LOFGREN. Well, let me get back to the statute. And I really think that if it is in a closed session or not, we ought to at least see the decision that has been discussed.

Mr. WAINSTEIN. And I will tell you that we have discussed with a number of Members in closed sessions various——

Ms. LOFGREN. Not me, and I have been to all the closed sessions I was invited to, so—I would just like to focus in on 105(b), where—

and it has been talked about earlier, about surveillance "concerning" versus "directed at," and what is meant to be covered by the use of the word "concerning" as compared to "directed at?"

It is a much broader description. Was it inadvertent or was it intended? And if intended, what was it—what is intended?

Mr. WAINSTEIN. Well, I will say I am not sure exactly, you know, because this was put together with the input of very many people, so I can't sort of ascertain exactly what every sort of intent or rationale was underlying the selection of that word.

I will say, though, that I am not sure that actually it is that much broader than "directed at," if broader at all.

Ms. LOFGREN. So then you wouldn't mind going back to the more traditional "directed at."

Mr. WAINSTEIN. Yes, I don't—"concerning," by the way, was in our bill that we proposed back in April, so this wasn't something new that just got sort of sprung in the PAA.

I would be perfectly happy to take a look at that. I think that as I said, I think, earlier, I wouldn't be surprised if some of the dynamics here were that we needed to fill this intelligence gap, we wanted to use a term which we knew would allow the intelligence community to fill that gap, and was concerned that any sort of perceived narrower terms might not allow us to do that.

Ms. LOFGREN. Well, my time has expired. I will just say that I think the—as you know, I am sure, I did not vote for this act, because it is either poorly drafted or it is intentionally drafted to be over broad.

And I look forward to working with you because, as I say, there is unanimous agreement on solving the problem that you state, not unanimous agreement on an expansion.

And I yield back to the Chairman and thank him for his indulgence while my light is on.

Mr. WAINSTEIN. Mr. Chairman, may I just follow up for a quick second? I think that raises an interesting issue, and we heard something from one of your colleagues about hypotheticals.

And the question is this, the reasonable reading of the statute—you know, those of us who went to law school—many of us heard, you know, the old lesson about, what if there is a law that says you can't have cars in a park.

But then someone has a heart attack in the park, and then the ambulance comes onto the park to get the person who has a heart attack. Does the ambulance driver get prosecuted for violating that law?

Well, obviously, that is not a reasonable reading of that statute. But that statute might not actually have a carve-out for ambulances, at least not explicitly.

So I think any statute you look at, like we are here—while I think this is a healthy process, any statute you look at, you can look at the margins and see whether, you know, potential scenarios could actually become a reality.

And the question is whether they are reasonable or not. And so while I agree that this is an important process to go through, that was the purpose of our letter to you of last week, is to tell you what we think is the reasonable reading of the statute.

Mr. CONYERS. Thank you.

Mr. WAINSTEIN. Thank you, sir.

Mr. CONYERS. I thank the gentlelady.

The Chair recognizes the distinguished gentleman from Indiana, Mike Pence.

Mr. PENCE. Thank you, Mr. Chairman.

And may I also add my words of appreciation to you for your strong and even-handed application of the rules of decorum in the hearing today?

And I appreciate this panel of witnesses and regret the circumstances under which you came before the Congress today.

And I particularly want to commend our second Director of National Intelligence, Director McConnell.

Your service in this role since February and your previous service in uniform, as well as the director of the National Security Agency under President Clinton is a record of service that speaks for itself, and I am grateful for your expertise in these areas.

As we say in Indiana, you have forgotten more about this area than I will have time to learn. But I am trying.

And, Mr. Wainstein, thank you for your testimony as well, and the balance of our panel.

If I could focus two quick questions, and I will ask them in succession, and then the witnesses can address them.

To Director McConnell, specifically, at a hearing 2 weeks ago on this subject, one witness, if you will recall, suggested that it was easy to tell when a foreign terrorist enters the United States, that you could simply look at billing records, see how much they are charged for phone calls. Surely it can't be that simple.

My question to you is can foreign targets move locations with little detection? Why is it difficult to pinpoint their location?

And could you respond to that in connection with the provision in the Protect America Act where we have broadened to include people reasonably believed to be outside the United States? How easy is it to know where someone is?

And let me leave that hanging and let you think about that, Mr. Director, if I can.

Secondly, very direct question, Mr. Wainstein. Can you clarify something for me? I have been in and out of the hearing today—other obligations. But I believe this came up earlier.

Particularly in light of some of the theatrics that went on today, it might even be more relevant to clarify. Does FISA either in its current form or in its preexisting form allow the Government to target the U.S. person for surveillance based upon antiwar statements?

In other words, can a U.S. person be designated an "agent of a foreign power" based on their antiwar statement? I have some recollection that there are specific provisions of the law to the contrary, and it seems like earlier in the hearing you were attempting to clarify that aspect of the law, and I think it would be a very, very important statement to make.

Mr. Wainstein, you might answer that directly, and then if the director can bat cleanup, that would be great.

Mr. WAINSTEIN. Thank you, sir. Yes, what I cited is a provision in FISA that in order to procure a FISA order the showing by which we establish that a person is an agent of a foreign power or

a foreign power—it can't be based solely on that person's exercise of his first amendment activities.

Mr. PENCE. Cannot be based.

Mr. WAINSTEIN. Cannot be. And then in the Protect America Act, under 105(b), as I said, there are five requirements that the Director of National Intelligence and the attorney general have to find before authorizing a surveillance, and one of them is that a significant purpose of the acquisition is to obtain foreign intelligence information.

So in other words, you have got to have legitimate foreign intelligence purpose. You can't just have political purpose in order to do it. Plus, it has to concern persons outside the United States.

Mr. PENCE. So specifically the law says that an individual may not be designated an agent of a foreign power for the purposes of surveillance simply based on the exercise of their first amendment rights, antiwar statements or otherwise.

Mr. WAINSTEIN. FISA does that, yes, sir.

Mr. PENCE. Okay. I may disagree with what people say. I will fight to the death for their right to say it. And I was under the impression that this act, as amended, was very clear on this point.

Director McConnell, on my first question about location and how easy it is to track where people are relative to surveillance?

Mr. MCCONNELL. Sir, in the old days, Cold War days, location was much, much easier. Today, with mobile communications, it is more difficult. So a target can move around.

There are some keys that can assist, but we can't know for certainty. One of the questions you asked was about billing records. If you had access to them, that may give you a clue.

But we probably wouldn't have access to the billing records, and if we had to have absolute certainty, it would put us in a situation where we couldn't keep up because the issue of having now to obtain a warrant.

So the evolution of communications over time has made it much more difficult. So what we were attempting to do is get us back to 1978 so we could do our business and legitimately target foreign targets, and keep track of threats and respect the privacy rights of Americans.

If there was some need for foreign intelligence with regard to a U.S. person, you have a warrant.

Mr. PENCE. And the standard of a person reasonably believed to be outside the United States was an effort to recognize——

Mr. MCCONNELL. Yes, sir.

Mr. PENCE [continuing]. The ambiguity of current technology.

Mr. MCCONNELL. Because a cell phone, for example, with a foreign number, GSM system, theoretically could come into the United States and you wouldn't appreciate that it had changed.

So you would have to now work that problem, and if you did then determine that it is in the United States and you had a legitimate foreign intelligence interest, at that point you have to get a warrant.

Mr. PENCE. Thank you, Chairman. I look forward to the closed session.

I thank the witnesses for their responses.

Mr. CONYERS. Thank you, Mr. Pence.

The Chair recognizes the gentleman from Massachusetts, Mr. Delahunt, Member of this Committee as well as the Foreign Affairs Committee.

Mr. DELAHUNT. Thank you, Mr. Chairman.

And I want to be very clear, because there has been some statements which would suggest that there are some that don't hold you, Mr. McConnell, and you, Mr. Wainstein, in the highest regard.

I think the concerns that you hear expressed are not ad hominem to you. They are not personal. They are institutional. They are what makes democracy function.

Should we trust Government? Well, the FISA Act came about because of abuses. All through our history there have been abuses. America was founded on a theory that executive power ought to be restrained and checked and balanced.

And that is what we are about here today. This isn't about working on the margins. This is something very fundamental to American democracy, from my perspective, and I think that is shared by everybody on the panel. That is why this is a serious hearing.

And let me respectfully take issue with you, Mr. Wainstein, when you describe ample oversight. Ample oversight has not been practiced until recently in this Congress. It just has been nonexistent.

We have reasons to be concerned when disclosures were made in the New York Times about the TSP and no member of this panel, despite having questions posed, was informed, Republican or Democrat.

So when we talk about oversight, it has been lacking. This is not the kind of protection, particularly when you have a single party in control of both branches of Government.

You know, divided Government probably is, in a democracy, necessary to protect our values and our institutions. But it hasn't existed.

The FBI Director appeared before this Committee for the first time—for the first time—since he was sworn in, I think, about 2 months or 3 months ago. That is not adequate oversight.

Do not rely on congressional oversight to serve as a filter for the actions of the executive branch. I am sure we all would trust you as individuals, but that is not what this is about.

You know, we read the newspapers. We understand the Deputy Attorney General went to the hospital to see a bed stricken Attorney General to debate a significant concern that he had about the functioning of the Department of Justice. So this is not working on the margin, with all due respect.

And, Director McConnell, you know, I hear you, and you talk about 200 hours and the work and the time that is invested in the preparation of an application for a FISA warrant.

Well, is it fair to say that just simply the work that would be done to secure your approval and that of the Attorney General would be significant and substantial as well?

Mr. MCCONNELL. Sir, the point I was trying to highlight is the fact that the interpretation of the old law was requiring us to get warrants for foreigners located in a foreign country——

Mr. DELAHUNT. Right.

Mr. MCCONNELL [continuing]. Introduced a series of actions that we just couldn't keep up. So by changing the law, which was done in August, we wouldn't have to go through that process for a foreigner in a foreign country.

We can keep up with anything that is done within the confines of the United States where it is foreign surveillance, and we have to have a warrant, so that is——

Mr. DELAHUNT. Okay.

Mr. MCCONNELL [continuing]. A manageable problem.

Mr. DELAHUNT. But let me ask you this. I mean, what I am hearing is it is an issue of resources. You know, I would suggest to you there is a willingness on the part of Congress, I believe, to give you whatever resources are necessary so that you can adequately respond.

There is not a single Member on this panel that does not want to give you what you need. And at the same time, we want to continue to ensure that fundamental freedoms, as we know them in a historical context, are being protected.

Mr. MCCONNELL. Sir, I am also as concerned as anyone about the fundamental freedoms and protection. And it wasn't a matter of resources. It was just the process to try to do our business.

And meantime, what I was trying to highlight in my comments, to provide context, was being required to have a warrant for a foreign target in a foreign country, by dint of the fact technology changed. That was the issue.

Mr. DELAHUNT. Right. My point is there is no disagreement as to dealing with the issue of the technology.

Mr. MCCONNELL. All the rest of——

Mr. DELAHUNT. It is unanimous.

Mr. MCCONNELL. All the rest of that was just explanation so you could understand——

Mr. DELAHUNT. Okay. Well, like I said, everybody is on board in addressing the technological issues here.

But there have been reports in the newspaper about the number of applications to the FISA court numbering in the tens of thousands. An almost negligible number—I remember when we were debating these and similar issues maybe a year or two ago. I think there were 15 or 17 that were denied by a FISA court judge.

Again, maybe it is that I am not on the inside understanding completely the process that you talk about and the work that is necessary. But I dare say that securing a FISA warrant, with all due respect to the FISA court, is much more perfunctory than I think the impression that you are leaving.

Mr. MCCONNELL. Sir, the conditions of the court—and remember, this is foreign intelligence——

Mr. DELAHUNT. Right.

Mr. MCCONNELL [continuing]. Is to demonstrate it is a foreign power or an agent of a foreign power.

Mr. DELAHUNT. Right.

Mr. MCCONNELL. And so the conditions are external, no warrant, external to the United States; internal, requires a warrant. So you wouldn't expect there would be very many turn downs. The process ensures it is legitimate, it is consistent with the law and so on.

But you are only proving one of two things, foreign power——

Mr. DELAHUNT. I understand that, but I guess what I am saying to you is, that is done in the normal course of the work of the intelligence community.

Mr. MCCONNELL. Yes, sir, it is.

Mr. DELAHUNT. This is not an additional burden.

Mr. MCCONNELL. True, it is not.

Mr. DELAHUNT. Therefore, it is an issue of resources.

Mr. MCCONNELL. Sir, the intent of the act in 1978 was to allow us to do foreign intelligence—remember 1978, Cold War, Russians, Chinese, North Koreans. It was to do that mission unencumbered by any process.

And so all we were attempting to do is get back to doing a foreign intelligence mission, so we are not spending time and energy and resources in the FISA court.

So all that I was giving with regard to the hours and so on is illustrative of what we were running into. The fundamental point is we shouldn't be required to have a warrant for a foreign target in a foreign country.

Mr. POWELL. And there is a very important substantive difference. Under FISA, we are required to make a probable cause showing that the person is a foreign power or an agent of a foreign power and reasonably going to use the facility that is targeted.

We do not do that for our overseas collection. We do not make probable cause showings for the thousands upon thousands of foreign intelligence targets.

The problem we had is, in fact, we were at a place where we were, in fact, in a large number of the workload given to the FISA court, making probable cause showings that people located overseas were agents of foreign power.

So it is not just a question of resources. It is a question of whether that is the appropriate substantive standard, which was not in anyone's contemplation according to the 1978 act, whether we want to be in a place where we are giving probable cause protection, something derived from the fourth amendment, to people located overseas.

And it was a large percentage of the FISA court workload that we were making these probable cause showings. And let me be very clear. It is not what our intelligence professionals do when they are doing overseas collection.

They do not make probable cause showings. They make a determination that it is a valid foreign intelligence target and it meets one of the requirements that is laid out.

So when intelligence agencies have limited resources, they know what the targets that they need to collect against are. And if it is a valid foreign intelligence target, they have a process for doing that.

There is no comparison between that process and the probable cause showing and the court process that we go through with FISA.

However, we were in a place where, in fact, we were doing that for foreign intelligence targets located overseas in a significant number of cases.

Mr. MCCONNELL. It is always useful to put some meaning on that kind of dialogue. Let me give you an example: American soldiers captured in Iraq by insurgents.

And we found ourselves in a position where we had to get a warrant to target the communications of the insurgents. That is how the process had evolved to put us in an untenable position.

Mr. WAINSTEIN. And if I could just add a little more context, it is not necessarily always an easy thing to establish probable cause of a connection between a person and a foreign power.

And you can go back and look at the 9/11 Commission where it details the difficulties they had in making that showing regarding Moussaoui and how that slowed up the ability to do a search with him.

So that is not always an easy thing to do.

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

Before we recess for votes and the very diligent witnesses have a break and hopefully a luncheon, I will recognize Judge Louie Gohmert from Texas.

Mr. GOHMERT. Thank you, Mr. Chairman. I didn't know if the Ranking Member had a question he needed to ask.

Mr. SMITH. The gentleman from Texas has been very patient. I wanted him to ask questions first, and I will come back and ask my questions after the break.

Thank you, though, for considering that.

Mr. GOHMERT. All right. Thank you.

There are a number of things that have triggered questions. First of all, I am sure you are aware of the problems, the abuses, that were outlined by the inspector general about national security letters.

And I am curious. Before the FBI uses national security letters, is there any process where they work with you or other Federal agencies to determine who is a foreign terrorist or foreign operative? I am curious.

I am just wondering what kind of interplay we have here among the agencies.

Mr. WAINSTEIN. Right. I don't know that there would be any interplay necessarily on that particular issue. In order to issue a national security letter, they have to show that it is relevant to an international terrorism investigation, let's say.

I can tell you that there is a good bit more scrutiny on that process within the bureau. They set up a compliance program, a compliance office, that is one of the main topics they are looking at.

Our division, the National Security Division, has set up an oversight unit, and we are going out and doing reviews of all the——

Mr. GOHMERT. And is that entirely an NSA unit? Because that flips over to my next question. Does the NSA vet or talk with the FBI or other Federal agencies about whom you believe may be a foreign terrorist?

Mr. WAINSTEIN. Just to clarify, and I will turn it over to Director McConnell, I head up what is called the National Security Division within the Department of Justice. So we work closely with the FBI on oversight matters.

In terms of the NSA——

Mr. MCCONNELL. Sir, there is very close coordination between the FBI and NSA on what is a terrorist and who they are and so on, so that goes on all the time.

Also, I would mention that the FBI now has a role under the DNI, because additional intelligence responsibilities under the act, Intelligence Reform Act of 2004, have been added to the FBI. So it was reasonably robust earlier. It is even more robust now.

With regard to national security letters, is a little different context. FBI has access to the information, but I don't know if there is any dialogue between NSA and FBI about using a national security letter.

Mr. GOHMERT. Because in a discussion like we are having, when you say, "Well, foreign agent, foreign soil, okay," then the question of who is a foreign agent, who works for a foreign terrorist operation becomes critical.

And you say you work together all the time, but does that mean it is required before a designation is placed on someone?

Mr. MCCONNELL. Yes. If you were going to get a warrant for surveillance, electronic surveillance, physical search, anything of that nature, there would be very close coordination.

National security letter is in a little different context.

Mr. GOHMERT. Well, but I am not talking about NSLs at this point. We have been talking about wiretapping.

Mr. MCCONNELL. Right.

Mr. GOHMERT. And before you put a wiretap on some foreign terrorist——

Mr. MCCONNELL. Close coordination.

Mr. GOHMERT. Close coordination. In every case.

Mr. MCCONNELL. Yes, sir.

Mr. GOHMERT. So that there is not information the FBI has about some foreign terrorist or the CIA has that the NSA has not accessed and reviewed in making the determination to wiretap a foreign terrorist without a warrant.

Mr. MCCONNELL. It may be theoretically possible, but the Intelligence Reform Act—the intent of that was to make that unlikely.

Mr. GOHMERT. Oh, I know that was the intent, and that was placed on there before I went. I am still concerned that we added a level of bureaucracy and didn't really fix anything. But that is a whole other discussion.

As I understood you—and again, Admiral, I appreciate your service. I appreciate all your services, even the naive comments from Mr. Wainstein about what is reasonableness in law school, because as I understand it, we don't let ambulances go into some wilderness areas even if it saves a life, you know, so what is reasonable in law school isn't really reasonable in the Federal Government.

But with regard to your testimony, I understood you to say no American has been wiretapped under the FISA program, is that correct?

Mr. MCCONNELL. Sir, my period of time starts in my confirmation in February, so I have been paying very close attention to that.

Mr. GOHMERT. All right, and that was—I was trying to get a time frame. Since February that is the base——

Mr. MCCONNELL. That is when my knowledge base starts.

Mr. GOHMERT. Okay, and that includes not merely NSA but CIA and FBI. Is that your understanding?

Mr. MCCONNELL. That is correct. Right. The issue we faced was because we were being required to get warrants, and it takes time——

Mr. GOHMERT. Sure.

Mr. MCCONNELL [continuing]. We actually took things off coverage. So the answer that I gave was correct.

Mr. GOHMERT. And because of concerns about the Federal Government, sometimes we notice it is not perfect, but are you aware of any wiretap under FISA ever being placed on the wrong number so it was tapping an American?

Mr. MCCONNELL. Occasionally there are mistakes, and then the process and the review you——

Mr. GOHMERT. Well, that is what I wanted to be sure, because I didn't hear any exceptions, and——

Mr. MCCONNELL. There have been some, yes, sir, and then you——

Mr. GOHMERT. Okay.

Mr. MCCONNELL [continuing]. Went and reported it and analyzed the case and that sort of thing.

Mr. GOHMERT. All right.

And I see my time has expired, and I would like to thank the Chairman. And by the way, when you were talking earlier about, Mr. Chairman, your concern for Americans who wanted to be abroad, I was concerned you were using slang to take us back to a discussion about the hate crimes bill.

I am glad to know that wasn't the case. But thank you for your time.

Mr. CONYERS. Thank you so much.

And I thank the witnesses for their endurance, and we will return after the votes. The Committee stands in recess.

[Recess.]

Mr. CONYERS. The Committee will come to order. We thank you for your patience.

The Chair recognizes the gentlelady from Wisconsin, Tammy Baldwin.

Ms. BALDWIN. Well, thank you, Mr. Chairman.

Thank you to our patient witnesses.

Rule 10 of the Rules of the House of Representatives sets forth the jurisdiction of the various standing Committees, and also sets forth their general oversight responsibilities.

And the Judiciary Committee has within its jurisdiction many elements, including the judiciary and judicial proceedings, civil liberties and Federal courts.

But I have to tell you, and I am sure it won't come as any surprise, that it is very challenging and often frustrating to thoroughly oversee a program many details of which are classified, and must be. I certainly understand that.

And it is even more challenging, in fact, sometimes impossible, to oversee secret programs, the existence of which Congress doesn't even know about.

So I just wanted to ask a few, I hope, general questions to help me satisfy myself that the scope of our current FISA oversight is adequate.

Now, we know today that in the weeks following the September 11 attacks in 2001, the President signed an Executive order setting up a secret surveillance program known as TSP, or the terrorist surveillance program.

And this, of course, has come to light in a very public way over the last couple of years. And I wonder if you are familiar with the Executive order in its entirety that set up that program.

Admiral, yes?

Mr. MCCONNELL. I am not. When I agreed to the nomination and was being considered, it was in the first week in January, and as I was going through the process, a decision was made to take the entire program and submit it to the FISA court.

So I have heard stories and I am generally aware, but I focused all my time on the period with the FISA court. And my focus has been getting us to a point where we were doing foreign surveillance but we had the right kind of process for warrants and that sort of thing.

Ms. BALDWIN. Okay.

Mr. MCCONNELL. So I don't know as much about the past.

Ms. BALDWIN. Okay. Well, so this is exactly, I think, a point that I want to make sure that I understand. You came in January 2007. At that point in time, there had been agreement that they were to take TSP and it would comply fully with FISA.

Are you aware that there were any other parts of that original Executive order setting up this TSP, the terrorist surveillance program, that were still going to be operating independently of FISA?

Or is the TSP the sum total of that original Executive order as you know any details about it?

Mr. MCCONNELL. No, ma'am. Everything that has to do with us, this community, conducting surveillance, foreign surveillance, for the purposes we have been discussing has been subjected to the FISA court and is being operated under the authority of the FISA court.

Ms. BALDWIN. And just for additional clarity, I know that several months ago—I think it was perhaps Attorney General Gonzales' last appearance before the Senate Judiciary Committee, as they were discussing the content of discussions with then-Attorney General Ashcroft in the hospital, he seemed to say in his testimony that the discussion in that hospital room was not about TSP but some other aspect of that original Executive order.

And maybe there is a way I should rephrase it. Does that Executive order have a date or a number that we can make sure we are talking about the same thing?

But in any event, he seemed to imply that there were other components that he was trying to seek authorization for. And I see Mr. Powell nodding his head. Maybe he has some information that can help clear this up.

Mr. POWELL. Yes. It was my understanding it was not an Executive order. It was what we call a presidential authorization. There was no secret Executive order that was signed.

The DNI sent a letter to Senator Specter and Senator Leahy on July 31st of 2007—I believe that was also publicly released—where he talked about, shortly after 9/11, the President authorized the NSA to undertake various intelligence activities.

A number of those activities were authorized in one order, which was reauthorized by the President approximately every 45 days. So there were a number of those orders with certain modifications.

One particular aspect of those activities was what the President expressed in December 2005. So there is a letter out there, that was just cleared by the community, discussing both those presidential orders and those activities and the reference to TSP, trying to bring some clarity to that. It is a confusing thing when we talk about these classified matters in open hearings.

Ms. BALDWIN. Right. And we are, shortly, I think, going to go into a classified hearing, and perhaps if there is anything you don't wish to share now and you can share it later, please just let me know, and I will go on a different course.

But I am familiar with that letter from the DNI. I have not seen it, and I don't have a copy, and I would love it for you to share it with me at some later point.

But, okay, they are saying in that that the TSP is one element of this presidential authorization now, not an Executive order.

Were there other elements that relate in any way to FISA or surveillance or warrantless surveillance that we should know about it in terms of fulfilling our oversight role with regard to FISA?

Mr. MCCONNELL. All of it is subjected to the FISA court and approved by the court, and we could take you into sort of the classified elements of it in a closed session.

Ms. BALDWIN. Okay. Is there a name for that presidential authorization that we are referring to, so that we won't get it confused with others? Is there a number or a name or a date that I should refer back to?

Mr. POWELL. We have just referred to it as a presidential authorization in my experience——

Ms. BALDWIN. Okay.

Mr. POWELL [continuing]. Just presidential authorizations.

Ms. BALDWIN. Okay. Are there other Executive orders or presidential authorizations aside from the one that we have just been discussing that in any way would bypass FISA for surveillance that we need? In terms of doing our oversight that we ought to know about?

Mr. POWELL. None that I am aware of. No.

Mr. CONYERS. The gentlelady's time has expired.

Ms. BALDWIN. And I would simply ask Mr. Wainstein if he has any further insight into this.

Mr. WAINSTEIN. Not that I can think of right now. No, not that I am aware of, I don't think.

Mr. CONYERS. The Chair now recognizes the Ranking Member of the Judiciary Committee, Lamar Smith.

Mr. SMITH. Thank you, Mr. Chairman. Mr. Chairman, first of all, I would like to ask unanimous consent that an editorial in today's *Wall Street Journal* on the subject at hand be included in the record.

Mr. CONYERS. Without objection, so ordered.

[The information referred to follows:]

The Wall Street Journal
The Wiretap Flap Continues
By BRUCE BERKOWITZ
September 18, 2007

One of the quirks of modern telecommunications is that a message from, say, Peshawar, Pakistan, to Beirut, Lebanon, might easily travel over a fiber-optic cable that passes through the United States. That, in essence, is the reason for the recent flap between Congress and the White House over foreign surveillance "wiretaps."

American law has always assumed that most domestic communications are protected by the Constitution, but foreigners communicating abroad are not, and are fair game for U.S intelligence. Such intelligence is critical today to monitor terrorists and proliferators of weapons of mass destruction.

The problem is that our laws were not designed for today's technology. Until about 10 years ago most international communications traveled by satellite, and intelligence services could snatch them out of the air. Now this traffic is carried over a highly interconnected fiber-optic network.

This network extends over most of the globe, but much of it is concentrated in the U.S. Messages travel at the speed of light, so distance matters little. They use whichever path has available capacity, and so a lot of global traffic goes through links operated by American companies inside U.S. territory.

This fact raises a question that is at the core of the controversy over what constitutes a "domestic" communication. At least one judge interprets the Foreign Intelligence Surveillance Act (FISA, the law that regulates such intercepts) to mean that any message traveling over a cable on American soil is a domestic communication -- even when it is from one foreigner to another foreigner, and both are on the other side of the world.

Under this reasoning, tapping the link requires a warrant. Taken to its logical conclusion, because all telecommunications on the global network can potentially pass through U.S. territory, all intercepts on the global network might require a court order. At a minimum, any message collected off the net in the U.S. would require one.

The paperwork would be enormous, and that's why the program was temporarily shut down. The Bush administration and Congress agreed in August to allow it to proceed under the old understanding for another six months, and debate it again this fall.

The fact that Mike McConnell, director of National Intelligence, has described the program so candidly says something about what is at stake. He has been willing to discuss many of the details of what we have been doing so that everyone can understand why we need to keep doing it. (Mr. McConnell also served as head of the National Security Agency, which is responsible for collecting most foreign intercepts -- "signals intelligence" or "SIGINT.")

The Bush administration must accept part of the blame for the controversy. It initially tried to

assert the power of the president, arguing that it could simply declare that these communications were foreign intelligence and bypass the courts entirely. It was making a philosophical point when it should have been trying to preserve activities that have endured for three decades precisely because they enjoyed the support of a broad consensus.

But Congress gets part of the blame, too. Even when it understood the huge loss in intelligence that had occurred, some members refused to pass a law that would permit these foreign intercepts unless it included near-perfect written guarantees that no innocent U.S. person would ever have his or her privacy violated.

In any case, the best thing now is for everyone to focus on the task at hand, which is to pass a law that does what we all want: Ensure U.S. intelligence can monitor foreign threats, while preventing the gross abuses that often happened before FISA was passed in 1978. The legislation would be a minor modification of current law and would look like this:

First, U.S. intelligence should be able to target any foreign national who is outside the U.S. It should not matter where the message actually travels, what the technology is, or where it is collected. That is the main change that is needed.

Second, all U.S. persons -- citizens and legal foreign permanent residents -- should be protected. If an intelligence agency wants to target a U.S. person, it should be required to get a court order. If an intelligence analyst happens to find information about a U.S. person who has not been targeted, that information should be documented and sequestered -- "minimized," to use the legal vernacular. That's the current rule, and by most accounts it has worked.

Third, companies that cooperate with U.S. intelligence to intercept communications from foreign targets should be immune from lawsuits. If a company acts at the request of an authorized U.S. official, and can show that it made a good-faith effort to comply with prevailing law, it should not be penalized.

Finally, the law should aim at establishing basic principles for the new technological era, rather than try to identify every specific situation that might require an intercept or scenario that could lead to abuse. Intelligence officials know what they really require to do their mission, and legislators know how to write authorizing legislation.

A little accommodation from all quarters would help a lot and rebuild some much-needed trust. Let's get on with it.

Mr. Berkowitz, a research fellow at the Hoover Institution, is a former CIA analyst who is frequently a consultant to U.S. intelligence agencies.

Mr. SMITH. Thank you again, Mr. Chairman.

Director McConnell, I really just had one question for you, largely because I understand all the other questions I had prepared have already been asked in my absence while I was gone for an hour.

My one question is this. What oversight procedures have been implemented by you or the intelligence community to protect the civil rights, civil liberties, of the American people?

I know you covered this to some extent in your prepared testimony, but I think it would be worthwhile for us to get your response in a little bit more detail, and also for Members to hear the extensive oversight that you all have implemented to protect those liberties.

Mr. MCCONNELL. Yes, sir. I would be happy to go through that. There are actually four tiers of oversight. Let me just cover them quickly.

First is within the agency conducting the program, and that involves internal regulations, training, supervisory review, audits. Internal agency reviews is how we would describe it.

That is both internal, supervisory, general counsel separately, and then the inspector general of the agency. So that is first tier, within the agency.

Second tier is by outside agencies. That includes my office, includes my general counsel, Ben Powell.

It also includes our civil liberties protection officer, who is here with us today. That is his job, is to make sure there is no violation of civil liberties, so he watches it from that standpoint.

And we work with the Department of Justice, the National Security Division that Mr. Wainstein heads up, in a similar oversight process.

The third tier is the FISA court, because either we are subjecting a request for a warrant and getting approval if it involves a U.S. person, or even in a foreign context we subject the procedures of FISA court review.

And they will determine that we, in fact, can have reasonableness in our process for determining a person is overseas, and if they objected for some reason we would have to comply with their objection or address their objection.

And the fourth tier is the Congress. Of course, we have got two oversight Committees on the House and the Senate side that are classified level, and they can review all these details, and then also a level of oversight from this Committee, given, you know, interest in following up.

Now, that is sort of the tiered level—probably can put a little more meat on the bones by just describing what has happened since the 5th of August. The bill is passed by the Congress on the 4th of August. The President signed it on Sunday morning, the 5th.

Since that time until today, we have had nine very detailed reviews. Let me just quickly capture some of those for you. Within 72 hours of it being passed, Members of the House Oversight Committee staff came out to the agency.

There were eight analysts, oversight personnel and the attorneys, and they went through very detailed review.

On the 14th of August, FBI General Counsel briefed the House Intelligence Committee and also included a representative—DOJ's oversight Committee and my office to go through the details.

Twenty-third of August, implementation team comprised of 13 analysts and attorneys updated for House Oversight Committee staff members.

And then I could go through infinite detail, but at each iteration, it is the procedure. It is the process. It is the certification. And of course, all of that has been submitted to the FISA court, and the FISA court is now going through a similar effort.

So nine different times with Members of the Hill, either Members or staff, we have gone through detail. And our pledge is that we will make it open and we will answer questions and subject it to oversight in a most vigorous way.

Mr. SMITH. Thank you, Director McConnell, and thanks for your excellent testimony today as well.

Mr. MCCONNELL. Thank you, sir.

Mr. SMITH. I yield back, Mr. Chairman.

Mr. CONYERS. Thank you.

The gentlelady from Texas, Sheila Jackson Lee, who serves as the Subcommittee Chair on Committee on Homeland Security as well as an active Member of Judiciary.

Ms. JACKSON LEE. Mr. Chairman, thank you very much.

And I do thank the witnesses. It has been a long day, and let me express my appreciation for your time here.

Director McConnell, the leadership that you have to give and have given is much appreciated by this Committee and also the American people.

As the Chairman indicated, I am also a Member of the Homeland Security Committee. We thank the representatives from the NSA and the Department of Justice as well for your service to this Nation.

But I have to make it very clear, or I have to at least raise this concern, and I would like you to address it as you probably have done on a number of occasions, that one of the striking elements of 9/11, the horrific tragedy, loss of life and the awakening of America, was not the absence of intelligence but the lack of sharing the intelligence.

So that was a crucial element of our faulting, if you will, and the final response of the 9/11 Commission and subsequent work after that.

Our Committee, the Homeland Security Committee, and this Judiciary Committee, have taken the initiative to try and fix many of those ills, and I am very pleased to have the honor of serving with Chairman Conyers and his Ranking Member, who have looked at civil liberties, for example, and many times through the same pair of glasses.

But now we come to seemingly a parting of the waters, and let me lay a framework of my concern. We have a National Security Act of 1947 that has suggested that the Administration must keep our Intelligence Committees fully and currently informed.

Congress, I think, has had a difficult time being able to rely on information. To a certain extent, it has been incomplete information from this Administration.

And so you might understand the skepticism of this Congress representing the American people to now yield very important civil liberties under the auspices or pretenses of needing them for national security.

It is my understanding that the solving of the German bombing that occurred, the bombing at the airport, the London bombing at the airport just recently by physicians, did not have a non-FISA process. It was a process that had overlapping restrictions, and we secured that information.

So I would like you to address these questions as relates to the Protect America Act and in the backdrop of knowing that I will have great difficulty in passing any legislation that does not have the oversight of a FISA court concept.

But why should we allow the existing bill, for those of us who did not vote for it but its existence is now the law, when you have indicated that it is about collecting foreign communications, but in this bill you allow the collection of U.S. communications?

And I would ask the simple question, since this is something that relates to the average American—the bus driver, teacher, the volunteer hospital worker—is whether or not you think the Protect America Act allows you to direct someone with access to electronic communications to open up any facilities necessary.

And could they use the PAA to direct a landlord to let you into someone's apartment so that you could access his or her computer?

My concern is the stark and, I would say, obvious intrusion on the American public, innocent individuals who have no intent on doing us harm, and why a FISA process would not be the appropriate intervening process that would protect civil liberties but ensure the safety and security of America.

Director McConnell?

Mr. MCCONNELL. Thank you for your questions—excellent opportunity to respond and put some context around at least my understanding of where we are.

First of all, let me agree with you that 9/11 should have and could have been prevented. It was an issue of connecting information that was available.

I am not sure you were in the room at the time, but I quoted from the joint inquiry of Congress that looked back on this, and I want to highlight one thing. There was a terrorist. It was a foreigner. He was in the United States. He was planning to carry out the 9/11 attacks.

And what the 9/11 Commission and the joint inquiry found is that person communicated back to al-Qaida overseas, and we failed to detect it. So the way you framed your question is why should——

Ms. JACKSON LEE. But we had them under surveillance. If we had pursued——

Mr. MCCONNELL. No, we didn't. That is the point.

Ms. JACKSON LEE. We had some of them under—we had some knowledge of these activities. We had knowledge of the individuals who were training to take off in terms of flight training and were not getting any training to land. We did not connect the dots.

And if we connected the dots——

Mr. MCCONNELL. We did not connect the dots.

Ms. JACKSON LEE [continuing]. We might have gotten that individual.

Mr. MCCONNELL. I am agreeing with you. We did not connect the dots.

Ms. JACKSON LEE. All right.

Mr. MCCONNELL. So what we were attempting to do in this update to the legislation is put us back where we were in 1978.

The way you framed your question—we have authority now to conduct surveillance against a foreign target in a foreign country. The way you also framed your question is we could conduct surveillance of a U.S. person.

And I want to correct that impression. We cannot conduct surveillance of a U.S. person—that is not only a U.S. citizen but that is a foreigner who is in this country—unless we have a warrant to do so.

Now, what we will quickly get into in a dialogue, those that have studied it and closely follow this. Well, what about when a foreign terrorist, known terrorist, calls into the United States? That existed in the 1978 time frame. It exists today.

We have a procedure to deal with that. We would minimize it if a foreign terrorist calls in and there is no intelligence value. But what I would highlight is that might be, as it was in 9/11, that might be the single most important call we would get. It might be to a sleeper cell. It might be activating something.

So the way the law was constructed—illegal to conduct surveillance, or electronic observation, or physical search or anything that—any of the things you went through without a warrant if the target is in this country.

But what it does allow us to do is to conduct foreign surveillance, and how it might connect to a sleeper cell or something of that——

Ms. JACKSON LEE. You are talking about the previous law or the PAA?

Mr. MCCONNELL. Today I am describing the Protect America Act, PAA.

Mr. CONYERS. Would the gentlelady yield?

Ms. JACKSON LEE. I would be happy to yield to the gentleman.

Mr. CONYERS. I want to commend the Director for conceding that 9/11 could have been avoided. But our staff studies show that the reason it wasn't has nothing to do with the FISA court. There were miscues all along the line in several respects.

And I thank the gentlelady for yielding.

Ms. JACKSON LEE. I thank the gentleman for acknowledging an important statement. We appreciate Director McConnell's straightforwardness that the dots were not connected.

Mr. MCCONNELL. Can I offer an explanation?

Ms. JACKSON LEE. Pardon me?

Mr. MCCONNELL. Can I offer an explanation to follow up on the Chairman's comment?

Ms. JACKSON LEE. I would yield to the director.

Mr. MCCONNELL. Thank you, ma'am. I am not used to that.

This community was so focused, so focused on foreign, that we allowed ourselves to be separated from anything that was potentially domestic.

The training process, the regulations, the oversight was if it is foreign, it is okay. If it has anything to do with domestic, it is not something we are supposed to be concerned with.

So it wasn't prohibited in the law, but it was in the cultural growth of the community since 1978, and that is what we suffered from when we——

Mr. CONYERS. Yes, that translates to negligence.

Mr. MCCONNELL. Or interpretation of the law, or how the culture had evolved.

Ms. JACKSON LEE. May I just make a final point? I have a whole series of questions, but let me just make this—we are now contending with spy satellites, and I would think that the basic civil liberties community, due process community, rightly so, has to be up in arms.

And therefore, Director, you can understand the sensitivity to what you have said. I believe that you are absolutely right, that what we needed to do, and we suffered a tragedy because of it, is to strongly change the culture.

But the culture was not the culture of America. It was the culture of the intelligence community. We should not be faulted, meaning American citizens, because the intelligence community themselves seemingly prohibit themselves from engaging in surveillance and using the tools that we had for them to be able to use domestically.

My concern is whenever you take the bar away that gives protection to American citizens on their civil liberties and due process and take away the FISA court that has worked—that can work with updating the technology and updating, then, again, I think that we miscue and we open ourselves to another kind of culture, and that is a spiraling down of protecting civil liberties and civil rights.

We can do both, which is national security and, as well, protecting those civil rights and civil liberties.

Mr. CONYERS. I thank the gentlelady.

The Chair recognizes Betty Sutton, Ohio.

Ms. SUTTON. Thank you, Mr. Chairman.

And I thank you gentlemen for your testimony.

As I begin, I would just like to—you know, last week or a week or so ago we had a hearing on this subject, and it was restated over and over again the importance of trust in carrying out the difficult work that you all are charged with.

And to that end, I just want to clarify some of the things that I have heard here today and make sure that I am understanding them correctly.

There was a line of inquiry from the Chairman about when this bill was put through the process in August, and discussions went on, as they often do, I am sure, between legislators and Director McConnell as they tried to put together something that would accomplish our goals without sacrificing fundamental freedom.

And if I understood you correctly, were you saying that through the course of that discussion that you never substantively changed your position from the beginning sort of to the end?

Mr. MCCONNELL. I did not substantively change my position, no, ma'am.

Ms. SUTTON. Okay. I just wanted to make sure that I was understanding you correctly.

Mr. POWELL. I would just remind—we did change our position in the sense that our original proposal of April did not have any FISA court involvement for people reasonably believed, or foreign intelligence targets believed, to be outside the United States.

And in fact, in the course of those discussions, the position was changed such that we agreed to put our procedures for determining the foreign targets—that, in fact, they were foreign. We agreed to put them into FISA court review.

That was not part of our April bill, and that was something the director agreed to, I believe, on August 1st or 2nd, and put out a statement saying although he would prefer not to do it, to accommodate the interest of the Congress and the American people, to assure them, we agreed to go to the FISA court.

So that was a substantive change of position where we agreed to put those procedures to the FISA court, which is not something that was part of the 1978 act.

Ms. SUTTON. But in those final weeks and those final days as this was being perfected, if I understand you correctly, Director, there were only, from your end, revisions made that were technical and not really substantive in nature, is that correct?

Mr. MCCONNELL. That is true. When it became apparent that we were going to shift the process into a compressed time, and we had the increasing information with regard to the threat, what I did was to try to boil it down to three main points, which I have said before.

I would repeat them if they are useful to you—but was to say no warrant for a foreign target in a foreign country, a way to compel the private sector to assist us, because we would need their help, and to require us to have a warrant for anything involving surveillance against a U.S. person.

So that was the philosophical approach. A word or two or a technical change—the reason that I was accused of changing my position is I agreed philosophically to the points and was asked to agree to a draft that I hadn't read, and I said I can't do that until I read it, because as I mentioned earlier, if you change a word or a phrase, it can have unintended consequences.

So that is why we got into the last-minute flail.

Ms. SUTTON. Well, it appears that there were some distinctions between what you were thinking philosophically then—and others. But let me continue with another question.

We have heard a lot about—and I have seen, of course, the interview in the *El Paso Times,* and one of the things that has been raised here today is this idea that you disclosed that 100 or less U.S. persons were being surveilled under the FISA orders.

Was that information ever classified?

Mr. MCCONNELL. Probably at one level and detail it was classified. What I chose to do, because of the importance of this debate—it was my authority to do it—wasn't directed to do it; I just thought about it—was to try to put some context at a summary level in the discussion so that there was a point of reference, some context for the dialogue.

So what I said was thousands in terms of foreign surveillance, but when a foreigner had called someone—there is suspicion of a sleeper cell or whatever—and then we got a warrant as a result of that—that was the number I used, 100 or less, just to provide context.

Ms. SUTTON. Okay. Okay. And, Director, then am I correct in understanding that you actually declassified it in the course of that interview? Is that the process that took place?

What was the date and process that you used to declassify it? I mean, when did it happen?

Mr. MCCONNELL. It was when I did the interview. It was a judgment call on my part.

Ms. SUTTON. Okay, so information can be just—I just want to understand the process, because I don't know—can be declassified by you in the course of an interview as you see it selectively appropriate to do so.

Mr. MCCONNELL. The power is vested in the President. The President has delegated that authority to me. So I can make that judgment when I see it is appropriate.

Ms. SUTTON. Okay. Okay. We have heard a lot of discussion also today about minimization. I know I am running out of time, but if I could just ask you a quick question on that point.

The minimization—it occurred prior to the Protect America Act. It was an additional safeguard that existed in the law, is that correct?

Mr. MCCONNELL. It has been in the law for a long time, 1978, and it goes back even further than that on the criminal side.

Ms. SUTTON. Okay. But I hear you talking about it today as if it is a substitute for going through the FISA court to get a warrant, and I guess my question, then, goes back to the whole point of why did we ever require a warrant in the first place, because we have always had minimization.

Mr. MCCONNELL. Well, the issue is the target. If the target is U.S. person, you have to have a warrant. If the target is foreign, and it somehow—although more often than not, it has not, but it somehow involves a U.S. person, that is where minimization would be used.

It was put into the process in 1978. It worked well. And it is still in effect, been reviewed by the court and approved, so it is something we have always used.

Ms. SUTTON. Thank you.

Mr. CONYERS. I thank the gentlelady from Ohio.

Steve Cohen, Tennessee?

Mr. COHEN. Thank you, Mr. Chairman. And I am going to take up a little bit where Ms. Sutton left off.

Mr. Wainstein, you have testified that one reason we shouldn't worry about Americans being spied on as a result of surveillance without a warrant that is directed at persons overseas under the PAA is minimization procedures to handle the acquisition, dissemination and retention of incidentally collected U.S. person information. Is that true?

Mr. WAINSTEIN. Yes, I think that is a very important part of the protections, both under the PAA and under other collections as well.

Mr. COHEN. So people shouldn't have to worry if they are spied on incidentally because you will minimize what is done with the information, is that right?

Mr. WAINSTEIN. Well, I guess the way I would frame it is that minimization procedures were adopted—you know, they go back before 1978, but in the context of general signal intelligence overseas they were adopted.

They are applied rigorously. They are trained on in the intelligence community so that if you are legitimately targeting somebody overseas, that person calls somebody in the United States, that U.S. person information gleaned from that—that that U.S. person information is handled carefully so that, you know, the U.S. person's name and identifying information is stripped out unless that information is necessary to understand the foreign intelligence value of that information.

So it protects U.S. person information from being sort of disseminated and used in an inappropriate way. So I think it is a very important protection. And it is one that has existed for a long time, and the PAA does not change it.

Mr. COHEN. And you can assure us that these names, if they are picked up, aren't ever released in any way.

Mr. WAINSTEIN. Well, I think the minimization procedures—some are classified, some are not classified. But essentially, what they do is—and this is laid out, you know, in classified form, and we can provide copes to you of the ones that aren't classified.

But it says if you get this information, that it has to be retained in a certain way, it can only be disseminated under certain conditions, you can only disseminate the U.S. person identifying information if there is—if you need that information for the consumer of the intelligence to understand the foreign intelligence value of that information.

So it is a very sort of careful, sort of sequenced handling of that information, so that, yes, there are situations where the name Ken Wainstein might come up in a surveillance, and that name will end up in a report, intelligence report, because it is important that Ken Wainstein's name be included in that report to make sense of it.

Mr. COHEN. Mr. Wainstein, let me ask you this. *Newsweek*—and you are probably familiar with this—in 2006, reported that in a 2-year period the NSA supplied the names of some 10,000 American citizens to interested officials and other agencies that the NSA had obtained minimized information.

They kept it in their files. Are you familiar with that?

Mr. WAINSTEIN. I am not familiar with that specific report, I am sorry, sir.

Mr. COHEN. Do we have a copy? Can we put a copy of that *Newsweek* report in the record, Mr. Chairman?

Mr. CONYERS. Without objection, so ordered.

[The information referred to follows:]

Newsweek

Hold the Phone

Big Brother knows whom you call. Is that legal, and will it help catch the bad guys?

Mark Hosenball And Evan Thomas

NEWSWEEK
Updated: 11:14 AM ET Oct 16, 2007

In the difficult days after 9/11, White House officials quietly passed the word through Washington's alphabet soup of intelligence agencies: tell us which weapons you need to stop another attack. At the supersecretive NSA, the National Security Agency (also known as No Such Agency), the request came back: give us permission to collect information on people inside the United States. The NSA had been struggling, without much success, to listen in on terrorists who use cheap and easily available encrypted phones, and officials eagerly drew up a wish list, according to a participant in the discussions. This source, who declined to be identified discussing sensitive matters, said NSA officials did not really expect the White House to say yes to domestic spying. After scandals over wiretapping erupt-ed in the 1970s, the code breakers and electronic sleuths at the NSA had been essentially restricted to eavesdrop-ping on conversations between foreigners abroad. American residents and even most foreign visitors to the United States were off-limits to "Big Noddy," as NSA insiders call their giant "Ear in the Sky" surveillance capability.

But after 9/11, president George W. Bush wanted fast action. He believed that most Americans thought their government should do whatever was necessary to catch terrorists before they struck again. Though the details remain highly classified, the "National Security Presidential Directives" issued by Bush called for an all-out war on terrorism, including, it is generally believed, expanded electronic surveillance. Out went the old rules--a 1980 document called "U.S. Signals Intelligence Directive 18," which sharply limited domestic surveillance; in came a new, still dimly understood regimen of domestic spying.

Desperate times call for desperate measures. In times of war, open societies have been will-ing to accept the need for secret spy services. Americans now spend upwards of $40 billion a year on intelligence. Given a hard choice between security and privacy, most Americans would probably choose to sacrifice some of the latter to get more of the former. The harder question is whether the techno wizards at the NSA, overwhelmed by tidal waves of digital data, searching for tiny poisonous fish in a giant sea, can provide true security from another 9/11.

There can be no doubt that Bush correctly read the public mood in the days and weeks following the 2001 attacks. And had the president sent a bill up to Capitol Hill giving the NSA broad powers to wiretap and eavesdrop inside the United States, in all likelihood, the lawmakers would have shouted it through. But the president did not ask for public support. Instead, like most chief executives charged with running the modern national-security state, he chose the path of secrecy. True, the administration's spymasters confidentially briefed congressional leaders on the new eavesdropping program. But some of the lawmakers now claim they were confused, or misled, or somehow did not fully understand what the spooks were telling them. Perhaps the legislators weren't fully informed. Or perhaps they didn't really want to hear what they were told.

In any case, the story eventually, and inevitably, leaked. Last December, The New York Times revealed that the NSA had eavesdropped on thousands of phone calls between people in the United States and foreign countries without first obtaining warrants. Then, last week, USA Today reported that the NSA had amassed a vast database of billions of calls inside the United States--not the content of the calls themselves, but a record of when and to which phone numbers the calls were made and for how long. (The government did not ask the phone companies for names and addresses, but the simplest Internet search of a phone number can divulge that information.) The revelation was another blow to Bush, whose approval rating in the new news-week Poll dipped to 35 percent, his record low in the survey, and it may slow the administration's plan to find a CIA director who can restore morale at the beleaguered intelligence agency. The brewing scandal is likely to entangle the government and the phone companies that helped in a legal morass.

Administration officials have always insisted that any eavesdropping or "data collection" had

been narrowly focused on Al Qaeda terror suspects. It is hard to determine if the NSA goes on fishing expeditions. A senior administration of-ficial, who declined to be identified discussing classified matters, acknowledged to NEWSWEEK that the NSA had crunched through vast databases to help identify suspects who may have then been subjected to electronic eavesdropping, either without a warrant or under court order. This official claimed that the NSA program had helped gather evidence that had foiled terrorist operations, though the official would not be more specific. If the program "leads to one disruption of another 9/11, then it would be worth it," said the offi-cial. But other administration officials interviewed by NEWSWEEK questioned whether the fruits of the NSA program--which they doubted, though not publicly at the risk of losing their jobs--have been worth the cost to privacy. And many Americans naturally wondered whether Big Brother was watching or listening in ways that are still unknown. There are hints, for instance, that the government has been fishing the Internet as well as the phone lines.

In San Francisco, a privacy group called the Electronic Frontier Foundation has filed a lawsuit based in part on the testimony of Mark Klein, an AT&T technician for 22 years who claims he witnessed the construction of a "secret room" for the NSA at AT&T's San Francisco headquarters in early 2003. Later that year, Klein says, he discovered that cables from the secret room were tapping into massive volumes of Internet communication. Klein says he discovered similar operations in other cities on the West Coast, and now concludes that the NSA had created the capability of "vacuum-cleaner surveillance" of all data crossing the Internet. AT&T says it has always obeyed the law and worked to safeguard the privacy of its customers. The federal government has mostly remained mum, though at a Dec. 19 White House briefing, Attorney General Alberto Gonzales somewhat cryptically referred to "many operational aspects" of the eavesdropping program "that have still not been disclosed." After the USA Today story, President Bush told reporters, "We are not trolling through the personal lives of millions of innocent Americans."

Whether that is strictly true will likely be on the agenda this week as lawmakers on the Senate intelligence committee grill Air Force Gen. Michael Hayden, Bush's choice to take over the troubled CIA. Hayden ran the NSA before and after 9/11, when the agency was expanding its surveillance programs. "I have substantial questions about his credibility," Senate intelligence committee member Ron Wyden, an Oregon Democrat, told NEWSWEEK. He points to Hayden's public statements that the NSA monitored only international calls. "There was never any mention of establishing a domestic database," says Wyden.

Republicans defending Hayden's nomination can counter with some early polls showing that most Americans support expand-ed electronic surveillance to catch terrorists, even if it intrudes on their privacy. (Much depends on the wording of a poll question, of course, and later polls showed more skepticism. The NEWSWEEK survey found 53 percent agreed with the statement that NSA data collection "goes too far in invading people's privacy," while only 41 percent agreed that the collection program is "a necessary tool to combat terrorism.") Most legal experts seemed to agree that the government could collect a huge database of phone records without violating the Constitution's ban on "unreasonable searches and seizures." Still, the phone companies that cooperated with the NSA--AT&T, Verizon and BellSouth--will be hauled into court, accused by their customers of violating the arcane and murky restrictions of various federal communications laws. All of them have protested that they were complying with the law, though it has been noted that they were paid for their cooperation, and lawyers suing the phone companies will undoubtedly want to know if they were pressured by threats to withhold valuable federal contracts. One much smaller phone company--Qwest, based in the Rocky Mountain states--refused to turn over its call records, arguing that the NSA never satisfied the company's legal doubts about the agency's request.

Americans are not naive about the need to snoop at home and overseas. In 1929, Secretary of State Henry Stimson shut down a secret code-breaking operation called the Black Chamber by saying, "Gentlemen do not read each other's mail." But America's enemies are apt to play dirty, and during World War II and the cold war, the federal government decided, in effect, to play dirty, too--to steal secrets and eavesdrop, at home as well as abroad.

Washington spun a huge web of intelligence agencies with acronyms familiar (like CIA and FBI) and obscure (like NRO--for National Reconnaissance Office--to operate spy satellites). The attitude toward secret or "black" operations was, at first, rather "stiff upper lip" and Brit-ish. Policymakers did not want to know too much about what the spooks were up to. Presidents were protected by the doctrine of plausible deniability. They were supposed to be able to say, plausibly, that they really didn't know how that secret was stolen--or that a journalist's phone was tapped or that a foreign government was overthrown. If caught, American spymasters were supposed to fall on their swords and take responsibility.

Of course, blame-taking didn't quite work so stoically in practice. During the Watergate scandal, it emerged that the Feds had been carrying on a program of domestic spying, tapping phones and opening the mail of real and imagined enemies of the state. At the 1975 Church Committee hearings, intelligence officials squirmed and pointed fingers. New laws were enacted, including

the 1978 Foreign Intelligence Surveillance Act, which requires the Feds to get a warrant from a secret court before eavesdropping on foreign calls in and out of the United States.

The NSA was banned from any domestic espionage. At those 1975 hearings, Sen. Frank Church, the chairman of the committee appointed to investigate intelligence abuses, made a statement that today seems ominous and possibly prescient. The Idaho senator said he was most worried about the NSA. The secret agency's capabilities were so great they "could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything, telephone conversations, telegrams, it doesn't matter. There would be no place to hide."

The NSA does have vast capabilities. One senior U.S. intelligence official, speaking anonymously because of the sensitivity of the subject, told NEWSWEEK that the heat generated by the NSA's secret supercomputers has been so great that officials have been talking about carting in snow and ice to mask the machines from the prying sensors of foreign spy satellites.

But increasingly, there has been talk of the agency's "going deaf." The NSA had its best luck monitoring Soviet lines of communication--for example, a microwave transmission from Moscow to a missile base in Siberia. But the new enemy is more shadowy and elusive. In 2002, General Hayden told NEWSWEEK, "We've gone from chasing the telecommunications structure of a slow-moving, technologically inferior, resource-poor nation-state--and we could do that pretty well--to chasing a communications structure in which an Al Qaeda member can go into a storefront in Istanbul and buy for $100 a communications device that is absolutely cutting edge, and for which he has had to make no investment for development."

According to most accounts, the NSA remains behind the telecommunications curve. A December 2002 report by the Senate intelligence committee not-ed that only a "tiny fraction" of the NSA's 650 million daily intercepts worldwide "are actually ever reviewed by humans, and much of what is collected gets lost in the deluge of data." Hayden told news-week that year that the NSA had been slow to catch up to new technology, and that he was obsessed with turning the enemy's "beeps and squeaks into something intelligible."

One of Hayden's most ambitious initiatives was called Trailblazer. It was a program aimed at helping the NSA make sense of its many databases--to put them to use. By more efficiently locating and retrieving messages, Trailblazer could help the NSA "data-mine," to find patterns in the huge volume of electronic traffic that might help lead sleuths to a terror suspect. Instead, the program has produced nearly a billion dollars' worth of junk hardware and software. "It's a complete and abject failure," says Robert D. Steele, a CIA veteran who is familiar with the program. Adds Ed Giorgio, who was the chief code breaker for the NSA for 30 years: "Everybody's eyes rolled when you mentioned Trailblazer."

What went wrong? The NSA apparently tried a clunky top-down approach, trying to satisfy too many requirements with one grand solution, rather than taking a more Silicon Valley-like tack of letting small entrepreneurs compete for ideas. John Arquilla of the Naval Postgraduate School at Monterey, Calif., a renowned "network" intelligence expert, says: "The real problem Big Brother is having is he's not making enough use of the Little Brothers"--the corporations that have become expert at manipulating databases for commercial use.

"Data mining" has been a boon to credit-card companies that can match customers and products. It has also helped the Feds track drug dealers who constantly buy and throw away cell phones (the technology can monitor frequent phone-number changes). Identifying and tracking terrorists may be a taller order. For one thing, terrorists have learned not to even use phones. A computer disk or message between, say, Osama bin Laden and Iraqi insurgent leader Abu Mussab al-Zarqawi is hand-delivered. Some terrorists have learned to leave messages hidden in Web sites. Others are given passwords to go on the Web sites and find the messages. Since that process involves no electronic communication--no e-mail or phone call--the NSA is kept in the dark.

Effective data mining might have averted 9/11, notes Philip Bobbitt, who served as a National Security staffer in the Clinton administration. On Sept. 10, 2001, the NSA, monitoring pay phones in Qaeda-controlled Afghanistan, intercepted two messages, "The match begins tomorrow" and "Tomorrow is zero hour." No one knew what to make of these messages, which in any event weren't translated until Sept. 12. But the CIA and FBI had the identities of two of the hijackers, who had been linked to earlier Qaeda plotting, in the agencies' computers. "Had we at the time cross-referenced credit-card accounts, frequent-flier programs and a cell- phone number shared by those two men, data mining might easily have picked up on the 17 other men linked to them and flying on the same day and at the same time on four flights," Bobbitt recently wrote in The New York Times.

There are doubts within the upper levels of the U.S. government that the NSA, four-and-a-half years after 9/11, is any better equipped and run to piece together the next "Tomorrow is zero

hour" intercept. NEWSWEEK has learned that some top government lawyers were troubled by the NSA data collection and search program--not on legal grounds so much, but because they doubted its efficacy. A senior administration official who was involved in legally vetting the NSA program but declined to be identified discussing sensitive matters says that a crude cost-benefit analysis left him uneasy. The NSA program ran a risk of intruding on the privacy of Americans. There are always "false positives." National Journal's Shane Harris conjured up the example of a book agent who represents a journalist who once interviewed Osama bin Laden. A faulty pattern analysis could make him a terror suspect. To justify the risk of dragging such innocents into government investigations, there needs to be evidence showing a high probability of return on the investment--the prospect of actually catching a terrorist.

So far, the best catch the Feds have offered up is a truckdriver named Iyman Faris, who conceived a rather farfetched plot to cut down the Brooklyn Bridge with a blowtorch. (Faris was apparently identified by a captured Qaeda leader; it's not clear the NSA played any role.) Of course, intelligence services do not always brag about their successes, and one U.S. official privy to the intelligence tells NEWSWEEK that another attack on an urban area in the United States was averted as well. The official would not discuss the plot for fear of revealing NSA listening methods.

There has been at least some debate inside the administration over how much license to give the NSA. In the spring of 2004, senior Justice Department lawyers objected to warrantless eavesdropping. For several months, until new rules to safeguard privacy were adopted, the program was suspended. It is not clear whether the NSA's data-collection program was also put on hold or altered in some way.

The administration is not eager to air its internal debates. At the Justice Department, an internal watchdog, the Office of Professional Responsibility, began an investigation into whether DOJ lawyers had behaved unethically by interpreting the law too aggressively--by giving a legal green light to coercive interrogations and warrantless eavesdropping. But the OPR lawyers had to drop their investigation last week when the administration refused to give them the necessary security clearances.

Catching Al Qaeda or some shadowy terrorist offshoot before it strikes again will take all the tools of spy tradecraft--old-fashioned human intelligence (HUMINT) as well as signals intelligence (SIGINT) like electronic eavesdropping. It is frustrating to think how close the CIA and FBI came to stopping 9/11. After Al Qaeda bombed the American embassies in Kenya and Tanzania in 1998, local police managed to catch one of the would-be bombers who had decided not to commit suicide in the blast. The conspirator was turned over to American intelligence officials, who persuaded the man to give up the phone number of a Qaeda safe house in Yemen. The NSA began listening in on the phone line of the safe house. American agents were tipped to a Qaeda terror summit in Kuala Lumpur in January 2000. Two of the 9/11 hijackers--Nawaf Alhazmi and Khalid Almihdhar--were at that summit. Somehow, the CIA failed to hand over the identities of these two terrorists to the FBI in time for the slow-moving bureau to track them before they flew into buildings on 9/11.

That was a human error, but it was caused in part by the culture of secrecy that permeates the national-security state. The CIA and FBI are renowned for their turf wars and unwillingness to share secrets. It's hoped that intelligence reform and the shame of failure have prodded the intelligence agencies to share a little more. As the late senator Daniel Patrick Moynihan observed, during the cold war excessive secrecy did more to hurt national security than to help it. In an overly secretive world, assumptions go untested and rigorous thinking is stifled. The CIA, for instance, failed to predict the collapse of the Soviet Union, in part because agency analysts refused to reach out to outside economists and experts.

It is true, as the old World War II saying goes, that "loose lips sink ships." But by refusing to tolerate an open discussion of new rules post-9/11, the Bush team lost a chance to gain public support for the necessary trade-off between security and privacy. Figuring out how to track and find Internet-savvy terrorists is a daunting task. Government officials--even the superspooks of the NSA--need all the help they can get.

URL: http://www.newsweek.com/id/47703

© 2007

Mr. COHEN. Thank you.

The issue is that if you get the information, we have got to rely—there is no warrant involved here, right?

Mr. WAINSTEIN. Well, there are minimization procedures that do apply to FISA orders, yes, so——

Mr. COHEN. But there is no warrant if your target is foreign.

Mr. WAINSTEIN. Right.

Mr. COHEN. There is no warrant in that context, not now.

Mr. McConnell, let me ask you this. The police, as you well know—are you an attorney?

Mr. MCCONNELL. I am not, no.

Mr. COHEN. You don't need to be an attorney to know this. Yesterday was Constitution Day, and we all need to remember the Constitution, the fourth amendment and all those things.

The police can't come into your house without a warrant, look around, copy files, take things, whatever, and claim there was no violation of your rights just because they threw everything away or they restricted its use on their own initiative after they looked in your home and, without a warrant, violated the Constitution and went back to the station.

Wouldn't you agree that minimization can't cure the damage done to privacy when the communications are intercepted in the first place?

Mr. MCCONNELL. Could I just refer back to the—how I opened up my statement at the beginning? The fault of 9/11 is we had someone in this country calling a terrorist that we didn't collect the information on—terrorist overseas.

So the issue is protecting the country, and when we—our target is foreign, and it is incidental coverage, you have to think about who is the target and where is the target.

Mr. COHEN. You say that was, in your original testimony, that was somebody in Florida, right?

Mr. MCCONNELL. San Diego, I believe it was.

Mr. COHEN. And who did they call? You say a terrorist. Do we know that person was a terrorist at the time?

Mr. MCCONNELL. Overseas, yes, sir.

Mr. COHEN. We knew it. And we didn't do anything at all?

Mr. MCCONNELL. For whatever reason, we didn't connect the dots for that. Now, let me set up the situation, how it might happen today. Sleeper in this country we don't know about, some sleeper that has been here for years, and al-Qaida, some member that we know about, calls in.

The reason for the way it is set up is if they activate that sleeper we would have some way of knowing. We might prevent a 9/11, or a sarin gas attack in a subway or whatever it might be.

In the course of international communications, first of all, we would only be conducting surveillance if it has a foreign intelligence target interest. We just don't indiscriminately look at the world.

So we would have some reason to look at it, so if it is incidental, has nothing to do with intelligence, that is what minimization is. You just take it out of the database.

Mr. COHEN. Well, I want to thank you for your service to the country and particularly I believe you served when President Clinton was President, is that correct?

Mr. MCCONNELL. I did, yes, sir.

Mr. COHEN. Appreciate your service, sir.

Mr. WAINSTEIN. Mr. Chairman, may I just respond a little bit to that last question?

Very briefly, the question is one that has been posed before, and I believe Congressman Lungren addressed this earlier, which is, is minimization sufficient. Or should we have to go get a court order when we have a valid surveillance against one target, and that person talks to another person, a person in the United States. Should we have some sort of court order to allow us to get that communication.

And you analogized the criminal context just now. And actually, the same situation applies in the criminal context when we are getting wiretaps under title III for law enforcement cases.

If you get a wiretap authority against me, you go to a court, get an order to intercept me, I have a phone call with Ben Powell—law enforcement is allowed to collect that surveillance, collect that communication, without going to the court to get a separate order to authorize listening in on the communication with Ben Powell.

Rather, that communication is just minimized because he is a United States person. He might well be innocent. So the same thing—different minimization procedures, but minimization is used on the criminal side as well as on the foreign intelligence side.

Mr. COHEN. Thank you for your comment. And you weren't around during President Clinton's time?

Mr. WAINSTEIN. Yes, I was.

Mr. COHEN. You were? Well, I was going to thank you in spite of the fact that you maybe weren't, but I still thank you for your service, too. I don't want to discriminate.

Mr. WAINSTEIN. No, I was a prosecutor using title III.

Mr. CONYERS. Thank you.

Hopefully inquirer is the gentleman from Alabama, Mr. Artur Davis.

Mr. DAVIS. Thank you, Mr. Chairman.

Gentlemen, thank you for your patience. I think we have had the NBA rule on 5 minutes today—a little bit on the generous side, but I will try to stay in the 5 minutes. Let me try to hit three separate areas fairly quickly.

Admiral McConnell, you mentioned—you just reiterated, but you mentioned in your opening testimony that one critical event with respect to September 11 was the unintercepted phone call that you just described, and I certainly wouldn't dispute that in any way.

But isn't it also the case that in the mid 1990's or perhaps the late 1990's that the U.S. had picked up intel that al-Qaida had developed a fixation with airplanes and was interested in hijacking? Have I got that right?

Mr. MCCONNELL. I know generally about that.

Mr. DAVIS. All right.

Mr. MCCONNELL. I haven't gone back to study it.

Mr. DAVIS. Now, wasn't there also some intelligence in 2001 that Middle Eastern individuals had gone to flight schools, had paid

cash, had left the flight schools under mysterious circumstances? Wasn't that information or something like it also known?

Mr. MCCONNELL. That is my understanding.

Mr. DAVIS. Well, and I make that point simply because I know—or I assume you don't mean to just pull out the phone call in isolation as the critical missed event.

There were a number of critical missed events as I recall from the chronology around this episode.

Mr. Powell, you are nodding. I assume you would agree with that.

Mr. POWELL. I would agree that there were a number of parts in the chronology beyond, that involve a whole host of things.

Mr. DAVIS. So just in fairness, I know a few of my colleagues on the other side of the aisle at some point have made the point today, or they have kind of implied, that but for this particular unintercepted phone call that there could have been some prevention of 9/11.

And certainly, none of the three of you mean to hang your hat in isolation on that as being the critical event, do you?

Mr. MCCONNELL. No, not at all.

Mr. DAVIS. Okay. Thank you.

Mr. MCCONNELL. We could have done better as a community.

Mr. DAVIS. Okay. Let me turn from that, and I appreciate that candid admission on your part. Let me turn to section 105(a). And the Chairman raised this question earlier, and I am not sure I heard the answer, so I want to try it again.

The section 105(a) provision—nothing in the definition of surveillance shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States—obviously, a critical provision.

This is directed at any of the three of you. Do you understand the term "person" to refer only to targets of surveillance?

Mr. MCCONNELL. Sir, let me tell you the way I understand it, and then we will let the two folks that wrote the bill say what their real intent was.

It goes back to the—you have to read the law in context, and it is how you define electronic surveillance. So what that is attempting to do is to take the fact that someone is foreign, foreign country, and remove it from the definition of electronic surveillance, so it allows us to conduct the surveillance regardless of where we do the intercept.

What we had gotten trapped into with the old language was the fact we were doing it in the United States caused us to go through this FISA procedure when it wasn't the intent of the original law.

Mr. DAVIS. Well, I certainly understand that is a matter of interpretation, but let me just ask you, Admiral McConnell, do you agree that the term "person" refers to targets of surveillance as opposed to individuals about whom there may be no intel whatsoever, who may not be legitimately classified as targets?

Mr. MCCONNELL. I am not sure I understood your question. If there is a nexus here, it is for the conduct of foreign intelligence.

Now, I would go back to what is in the front part of the law with regard to protecting U.S. citizens and the U.S. citizen is not going to give away his fourth amendment rights.

Mr. DAVIS. Well, let me perhaps come at that a different way and perhaps get the lawyers to weigh in.

Do either of you accept that there is any constitutional limitation on the United States' ability to conduct surveillance abroad? Is there any constitutional limitation whatsoever?

Mr. WAINSTEIN. Well, certainly, if U.S. persons are involved——

Mr. DAVIS. No, no, I am talking about someone who is not a U.S. person, surveillance of someone abroad. Is there any limitation whatsoever on the Government's ability to conduct surveillance of someone outside of the United States?

Mr. MCCONNELL. If it is a foreign person outside the United States, there would not be a limitation.

Mr. DAVIS. All right, so you would——

Mr. MCCONNELL. Other than something we may have agreed to in a treaty or something like that.

Mr. DAVIS. All right. But you would concede a limitation on an American citizen who was abroad, is that correct, a limitation with respect to the Government's surveillance authority?

Mr. Wainstein?

Mr. WAINSTEIN. Well, it is a constitutional matter. Any search involving a U.S. person——

Mr. DAVIS. Okay.

Mr. WAINSTEIN [continuing]. Overseas has to be reasonable.

Mr. DAVIS. All right. What about someone who is a non-American, someone who is a not a citizen? Is there any constitutional limitation on the Government's ability to conduct surveillance against that person outside the United States?

Mr. MCCONNELL. Outside the United States.

Mr. DAVIS. Yes.

Mr. MCCONNELL. No.

Mr. DAVIS. And do the two lawyers agree with that?

Mr. WAINSTEIN. Yes, not under the fourth amendment.

Mr. POWELL. I don't know of one under the fourth amendment. There may be things by treaty or international obligations——

Mr. DAVIS. Okay. Well, not counting treaty or some specific statutory arrangement we may enter, is it the position of the executive branch that the United States government faces no constitutional limits on its ability to conduct electronic surveillance against a non-American who is outside the United States? Is that your position?

Mr. POWELL. There is some Supreme Court case law talking about if somebody has a substantial connection to the United States, so there are——

Mr. DAVIS. Okay.

Mr. POWELL [continuing]. Cases out there that may come into play. I am just trying to think through in my mind. There is a substantial connection——

Mr. DAVIS. Well, if I can stop you for 1 second, there is Supreme Court case law around this, and frankly, the Supreme Court case law is not exactly crystal clear. You just articulated one exception or one potential exception that exists.

The problem is the statute is very specific. The statute says a person reasonably believed to be located outside the United States.

There is no caveat or no provision in the law that Congress just passed—which, by the way, I voted for.

As I understand it, there is no provision in here which contains the U.S. Supreme Court exception you just described, am I right?

Mr. POWELL. Well, if it is constitutionally based, it would not need to be in the statute. I mean, we are still going to have—if there is a constitutionally based restriction, we would not——

Mr. DAVIS. Are you sure of that, Mr. Powell, because—and I don't want to prolong this, but it is a very important issue, I think.

The Administration's position was that the force authorization after 9/11 had implications for the Geneva Convention, that the force authorization after 9/11 had implications for FISA.

The Administration's position was that the authorization for the force authorization after 9/11 had implications for habeas corpus. None of those things are contained in the force authorization.

So I am a little bit concerned when I hear the executive branch saying well, you know, we say person, but we don't really understand it that way, because the Administration has had a very, very expansive tendency when it comes to interpretation of statutes passed by the Congress. I think you would all agree with that.

And again, while I have an enormous amount of respect for the service you are all making for your country, the lawyers for your Administration went before the Supreme Court and said that the 9/11 authorization allows the President to make habeas corpus suspensions in some instances.

That is nowhere in the legislative history and certainly nowhere in the language. So again—and understand, I say this as one who voted for the bill but wants to see it fixed in a few months—the term "person" is a very literal term.

In my mind, it seems to encompass any live human being. The Supreme Court has not interpreted the Government's powers so broadly.

And, Mr. Powell, if I heard you correctly earlier, several times today you have used the term "target," and with respect to section 105(a), you have said target. That word is not there. "Person" is there.

Do you understand "person" and "target" to be synonymous?

Mr. POWELL. When I use the term "target," I am talking about a specific selection that we have made——

Mr. DAVIS. Yes.

Mr. POWELL [continuing]. To surveille.

Mr. DAVIS. Right.

Mr. POWELL. And that is connected with a person in many cases.

Mr. DAVIS. But you are talking about not a random human being but someone who has been selected as part of the intelligence-gathering process.

Mr. POWELL. Correct. I am talking about somebody——

Mr. DAVIS. All right.

Mr. POWELL [continuing]. Who has been determined to be a——

Mr. DAVIS. Does this say that?

Mr. POWELL [continuing]. Valid foreign intelligence requirement—to meet a valid——

Mr. DAVIS. All right.

Mr. POWELL [continuing]. Foreign intelligence requirement. That is what we do.

Mr. DAVIS. Yes.

Mr. POWELL. That is what we spend money to do.

Mr. DAVIS. You are 100 percent correct. Does the bill say what you just said?

Mr. POWELL. Well, the bill says that we have to have a foreign intelligence purpose to be doing this, or we cannot do it, so the foreign intelligence limitation is there in the certification signed out by the DNI and the Attorney General.

Yes, that is in the bill that we have to have a foreign intelligence purpose to do it. We cannot do it because we have a——

Mr. DAVIS. Mr. Chairman, if I can just wrap up with this point.

I think what you have said, Mr. Powell, is the better, the more good faith, reading of the law. But I would submit to you it is not the literal reading of the law.

We have a U.S. Supreme Court that has at least five justices who profess to care very much about the literal statute. So let me ask you this way—and, Admiral, I would be happy to pose this question to you, perhaps to Mr. Wainstein, if Mr. Powell, you know, is unable to answer it.

Any problem with amending this statute when we come back in the next 5 months and being more specific about what "person" means?

Mr. MCCONNELL. Sir, I have no problem looking at any language, just, as I said to the Chairman earlier——

Mr. DAVIS. Right.

Mr. MCCONNELL [continuing]. As long as we can look at it in context, understand what is intended and what that unintended consequences might be, so we can do our job.

But where we were last time, it was last-minute changes——

Mr. DAVIS. Sure.

Mr. MCCONNELL [continuing]. And, you know, that is where we got into a bind. So as long as we do it open and look at it and understand it and I can agree to it, then I would be happy to do that.

Mr. DAVIS. Mr. Wainstein, any objection from the Department of Justice to being much more specific about what "person" means?

Mr. WAINSTEIN. We would have no objection to looking at what you would propose or what anybody would propose.

Mr. DAVIS. What is wrong with saying target?

Mr. WAINSTEIN. Well, I am not sure that there is anything wrong, frankly. I would have to take a look at it. "Person" is defined in FISA. It is one of the statutorily defined terms.

So I would have to sort of go look at the interplay of that and changing to the term "target." But no, as we have responded to a number of the questions today about certain terms in the statute, we are happy to take a look at them.

Mr. DAVIS. Well, let me just end on this point. Again, this may have sounded like a contentious argument, but I will tell you why it is not. What this Congress has been grappling with for, frankly, the last 7 months—the last several didn't care to grapple with it.

But what this Congress has been grappling with for the last 7 months is a pattern of taking statutes, or taking plenary presi-

dential powers, and giving them enormous latitude and, frankly, in some instances, doing it without any statutory predicate.

So you may understand why there is some resistance on this side of the aisle to you saying, "Well, everyone who understands the statute would reasonably interpret it this way." Some people would have thought that everyone who understood habeas corpus would reasonably interpret it a certain way.

And I think that is the trust point that Ms. Sutton was making earlier. We have extraordinary trust for you gentlemen as individuals.

Unfortunately, your Administration's constant tendency to push the edge of its powers leads us to wonder if this bill, which passed overwhelmingly in the Senate and got 41 of my Democratic colleagues in the House—I understand why some of my colleagues wonder if this bill will be interpreted in the way that it is meant to be interpreted. Your Administration's history leads us to wonder about that.

And I will yield back, Mr. Chairman.

Mr. CONYERS. I thank the gentleman for his important contribution.

I thank the witnesses for their tenacity and staying power and candor here today.

And I turn to the gentleman from California, Mr. Lungren, for the final comment.

Mr. LUNGREN. Oh. Well, thank you very much, Mr. Chairman. I appreciate that.

One thing I would say is that one of the guides about how the Administration may act is how it is acting. And as I can take it, you are enforcing this law right now, and we have this period of time to see how you do it.

But having said that, I would hope that we might take to heart some of the comments and questions of Mr. Berman from California in those areas where in the letter that we received from you, Mr. Wainstein, you indicated that that is not the intention of the Administration, that is not the way you interpret it.

And maybe we can sit down and get some language which specifies that it will not be used in those ways, which is the easiest thing for me to look at as not changing the essentials of what the admiral came to us with and why he indicated that the fix that was offered as an alternative he did not believe met the need.

Perhaps we can meet somewhere in the middle with respect to these kinds of clarifications without changing the essential bill that we passed into law just, what, one and a half months ago.

Mr. CONYERS. I thank the gentleman for his contribution.

We realize that this has been a very important hearing. We are going to review the record carefully. It seems that the bottom line is that there are a number of things that could be clarified to everybody's benefit.

And so we will, without objection, give all Members 5 legislative days for additional questions, and the record will remain open for those same 5 legislative days.

And with that, this hearing is adjourned.

[Whereupon, at 4:26 p.m., the Committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE LAMAR SMITH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS, AND RANKING MEMBER, COMMITTEE ON THE JUDICIARY

Thank you, Mr. Chairman.

The modernization of the Foreign Intelligence Surveillance Act is one of the most critical issues facing the House Judiciary Committee.

I am encouraged that we have the Director of National Intelligence, Michael McConnell, and the Assistant Attorney General for the National Security Division, Ken Wainstein, here today to provide the Committee with important information on the real world implications of FISA reform.

This is the first appearance of the Director of National Intelligence before the Judiciary Committee.

Director McConnell's intelligence and national security career spans over 30 years. He has served under both Democratic and Republican Presidents, including as the Director of the National Security Agency in the Clinton Administration.

Despite his impressive, non-partisan service in the Intelligence Community, his motives have been impugned simply because he supports a policy he believes in. Such partisan criticisms distract us from what should be a non-partisan issue—protecting our country from terrorist attacks.

Foreign terrorists are committed to the destruction of our country. We are at war with sophisticated foreign terrorists, who are continuing to plot deadly attacks. It is essential that our Intelligence Community has the necessary tools to detect and disrupt such attacks.

Foreign terrorists have adapted to our efforts to dismantle their operations. As their terrorist operations evolve, we need to acquire new tools and strategies to respond to their threats.

We have a duty to ensure that the Intelligence Community can gather all the information they need to protect our country.

In the 30 years since Congress enacted the Foreign Intelligence Surveillance Act (FISA), telecommunications technology has dramatically changed, and terrorists have employed new techniques to manage and expand their terrorist networks.

Before we left for the August recess, Congress passed important legislation to fill a gap in FISA.

We need to make that fix permanent and pass other measures needed to prevent another terrorist attack against our Nation.

FISA does not require a court order to gather foreign communications between foreign terrorists outside the United States.

The real issue is this: Should FISA require a court order when a known foreign terrorist communicates with a person inside the United States? The Intelligence Community and 30 years of experience under FISA say no. For the last 30 years FISA never required such an order.

Requiring a court order for every phone call from a foreign target to a person inside the U.S. is contrary to FISA and common sense—how can the Intelligence Community anticipate a communication from a foreign terrorist to a terrorist inside our country?

In much the same way as a criminal wiretap, FISA provides—and has provided for 30 years—specific minimization procedures to protect the privacy of persons inside the United States with whom a foreign target may communicate.

It is unclear why now, after all this time, some seek to dismantle rather than modernize FISA.

Requiring separate FISA authority for these calls could be a deadly mistake.

Calls between a foreign terrorist and a person located inside the United States should be minimized in accordance with well established procedures. To do otherwise is to jeopardize the safety of our Nation.

The Director of National Intelligence made it clear that FISA modernization is essential to the Intelligence Community to protect America from terrorist attacks.

The American people understand what is at stake—almost 60 percent of Americans polled on the subject of FISA reform supported the Protect America Act. Less than 26 percent opposed it. The simple fact is that Americans support surveillance of foreign terrorists when they contact persons in the United States.

I look forward to today's hearing with the hope that the debate on FISA reform will lead to enactment of all of the Director's proposals submitted in April.

These proposals would ensure assistance from private entities in conducting authorized surveillance activities, make certain that private entities are protected from liability for assisting the government, and streamline the FISA process so that the Intelligence Community can direct resources to essential operations.

These reforms are long overdue. They should be debated without exaggerated claims of abuse or unfounded horror stories of threats to civil liberties.

We should maintain our commitment to winning the war against terrorism.

We must do all that we can to ensure that the words "Never again" do in fact ring true across our country.

I yield back the balance of my time.

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS, AND MEMBER, COMMITTEE ON THE JUDICIARY

SHEILA JACKSON LEE
18TH DISTRICT, TEXAS

WASHINGTON OFFICE:
2435 Rayburn House Office Building
Washington, DC 20515
(202) 225-3816

DISTRICT OFFICE:
1919 Smith Street, Suite 1180
The George "Mickey" Leland Federal Building
Houston, TX 77002
(713) 655-0050

ACRES HOME OFFICE:
6719 West Montgomery, Suite 204
Houston, TX 77091
(713) 691-4882

HEIGHTS OFFICE:
420 West 19th Street
Houston, TX 77008
(713) 861-4070

FIFTH WARD OFFICE:
3300 Lyons Avenue, Suite 301
Houston, TX 77020

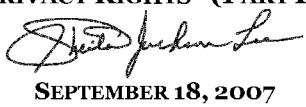
Congress of the United States
House of Representatives
Washington, DC 20515

COMMITTEES:
JUDICIARY
SUBCOMMITTEES:
COURTS, THE INTERNET, AND INTELLECTUAL PROPERTY
IMMIGRATION, CITIZENSHIP, REFUGEES, BORDER SECURITY, AND INTERNATIONAL LAW
CRIME, TERRORISM AND HOMELAND SECURITY
HOMELAND SECURITY
SUBCOMMITTEES:
CHAIR:
TRANSPORTATION, SECURITY AND INFRASTRUCTURE PROTECTION
COAST, MARITIME, AND GLOBAL COUNTERTERRORISM
FOREIGN AFFAIRS
SUBCOMMITTEES:
AFRICA AND GLOBAL HEALTH
MIDDLE EAST AND SOUTH ASIA
BLACK VOICE:
DEMOCRATIC CAUCUS
VICE:
CONGRESSIONAL BLACK CAUCUS
CHAIR:
CONGRESSIONAL CHILDREN'S CAUCUS

CONGRESSWOMAN SHEILA JACKSON LEE, OF TEXAS

STATEMENT BEFORE THE COMMITTEE ON THE JUDICIARY

OVERSIGHT HEARING: "WARRANTLESS SURVEILLANCE AND THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: THE ROLE OF CHECKS AND BALANCES IN PROTECTING AMERICANS' PRIVACY RIGHTS" (PART II)



SEPTEMBER 18, 2007

Thank you, Mr. Chairman for holding this hearing. Let me also welcome and thank our witnesses:

- The Honorable Mike McConnell, Director of National Intelligence
- The Honorable Kenneth Wainstein, Assistant Attorney General for National Security, United States Department of Justice

Mr. Chairman, the purpose of this hearing is to consider the concerns of non-governmental organizations and actors regarding the contours of the "Protect America Act," P.L. 110-55, S. 1927, a short-term revision to the Foreign Intelligence Surveillance Act that was passed by the Congress in the waning hours before adjourning for the August district work period.

I strongly opposed that legislation. Had the Bush Administration and the Republican-dominated 109th Congress acted more responsibly in the two preceding years, Congress would not have been in the position of debating legislation that has such a profound impact on the national security and on American values and civil liberties in the crush of exigent circumstances. Mr. Chairman, the circumstances attending the development, debate, and deliberation of S. 1927 illustrates the truth of the saying goes that "haste makes waste."

S. 1927, the cleverly named but misleading, Protect America Act, Madam Speaker, purports to fill a gap in the nation's intelligence gathering capabilities identified by Director of National Intelligence Mike McConnell, by amending the Foreign Intelligence Surveillance Act (FISA). But as I stated on the floor during general debate, in reality the bill eviscerates the Fourth Amendment to the Constitution and

represents an unwarranted transfer of power from the courts to the Executive Branch and a Justice Department led by an Attorney General whose reputation for candor and integrity is, to put it charitably, subject to considerable doubt.

Mr. Chairman, the Foreign Intelligence Surveillance Act (FISA) has served the nation well for nearly 30 years, placing electronic surveillance inside the United States for foreign intelligence and counter-intelligence purposes on a sound legal footing and I am far from persuaded that it needs to be jettisoned or substantially amended. But given the claimed exigent circumstances by the Administration, let me briefly discuss some of the changes to FISA I would have been prepared to support on a temporary basis, not to exceed 120 days.

First, I was prepared to accept temporarily obviating the need to obtain a court order for certain foreign-to-foreign communications that pass through the United States. But I insist upon individual warrants, based on probable cause, when surveillance is directed at people in the United States. The Attorney General must still be required to submit procedures for international surveillance to the Foreign Intelligence Surveillance Court for approval, but the FISA Court should not be allowed to issue a "basket warrant" without making individual

determinations about foreign surveillance. During wartime, I accept the need for an initial 15-day emergency authority so that international surveillance can begin while the warrants are being considered by the Court. But there must be meaningful congressional oversight, requiring the Department of Justice Inspector General to conduct an audit every 60 days of U.S. person communications intercepted under these warrants, to be submitted to the Intelligence and Judiciary Committees. Finally, as I have stated, this authority must be of short duration and must expire by its terms in 120 days.

In all candor, Mr. Chairman, I must restate my firm conviction – shared by millions of Americans -- that when it comes to the track record of this President's warrantless surveillance programs, there is still nothing on the public record about the nature and effectiveness of those programs, or the trustworthiness of this Administration, to indicate that they require any legislative response, other than to reaffirm the exclusivity of FISA and insist that it be followed. This could have been accomplished in the 109th Congress by passing H.R. 5371, the "Lawful Intelligence and Surveillance of Terrorists in an Emergency by NSA Act" (LISTEN Act)," which I have co-sponsored with the then Ranking Members of the Judiciary and Intelligence

Committees, Mr. Conyers and Ms. Harman.

I think the record also should reflect that the Bush Administration has not complied with its legal obligation under the National Security Act of 1947 to keep the Intelligence Committees "fully and currently informed" of U.S. intelligence activities. Congress cannot continue to rely on incomplete information from the Bush Administration or revelations in the media. It must conduct a full and complete inquiry into electronic surveillance in the United States and related domestic activities of the NSA, both those that occur within FISA and those that occur outside FISA.

The inquiry must not be limited to the legal questions. It must include the operational details of each program of intelligence surveillance within the United States, including: (1) who the NSA is targeting; (2) how it identifies its targets; (3) the information the program collects and disseminates; and most important; (4) whether the program advances national security interests without unduly compromising the privacy rights of the American people.

Given the unprecedented amount of information Americans now transmit electronically and the post-9/11 loosening of regulations governing information sharing, the risk of intercepting and

disseminating the communications of ordinary Americans is vastly increased, requiring more precise — not looser — standards, closer oversight, new mechanisms for minimization, and limits on retention of inadvertently intercepted communications.

Mr. Chairman, we must never lose sight of the reason why we permit the Executive Branch to conduct foreign intelligence surveillance. Congress has authorized this activity to assist the Executive Branch in protecting the American people from foreign countries, organizations, agents, and actors who seek to harm our country and change our way of life. Americans rightly are proud of their way of life because, at bottom, it is made possible by adherence to a shared consensus regarding the values and beliefs that make our lives so rewarding, so fulfilling, and so special that ordinary men and women gladly don the uniform and willingly risk life and limb to preserve it.

Mr. Chairman, every day the brave and heroic men and women of the Armed Forces stand on guard ready to defend their countrymen's liberty, including the right of privacy and their Fourth Amendment right to be secure in their persons, houses, papers, and effects. It would make a mockery of their devotion to preserving our way of life against

foreign adversaries if this Congress voluntarily surrendered those rights by vesting in the Executive Branch more powers than are overbroad, unnecessary, and virtually unlimited. Mr. Chairman, the Executive Branch should have all the power necessary, but only the power necessary, to protect the American people from foreign adversaries.

It is worth recalling that this country was founded on the bedrock principle that governments exist to secure the inalienable rights of humankind – life, liberty, and the pursuit of happiness – and that government derives its just powers from the consent of the governed. Given their horrid experience living under the yoke of King George III, the Framers had a healthy concern for the abuse of power by those who wielded executive power. It is for that reason they subordinated the Executive Branch to the Legislative Branch; it is no mere coincidence that Congress is created and empowered in Article I of the Constitution and the Executive Branch is addressed in Article II. In the Declaration of Independence Jefferson detailed the abuses, usurpations, and indignities suffered by the Colonies at the hand of an out of control executive. James Madison, the chief architect of the Constitution took great care to ensure that the Chief Executive would never be able to

exercise the absolute powers of a monarch.

It is the American way, Mr. Chairman, to be wary of any attempt to aggrandize power in the hands of the Executive. My concern with the so-called Protect America Act is that it breaks faith with this long-standing and cherished American value. I believe that delegating to the Executive sweeping powers to eavesdrop on Americans without a warrant or constitutional probable cause will in the end sacrifice our liberty without increasing our security. I am looking forward to discussing these matters in more detail with our witnesses.

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

PREPARED STATEMENT OF THE HONORABLE STEVE COHEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE, AND MEMBER, COMMITTEE ON THE JUDICIARY

I thank the Chairman for holding this additional hearing on the important issue of the harmful changes to the Foreign Intelligence Surveillance Act (FISA) wrought by the misnamed Protect America Act (PAA). These changes undermine FISA's core by removing from its protection a broad category of electronic communications, subjecting such communications to government surveillance without court authorization or oversight.

In addition to the substantive problems with the PAA, I am wary of the manner in which it was passed. Just prior to Congress's August recess, DNI Michael McConnell originally agreed that a less onerous version of the bill would be acceptable to him. At the eleventh hour, and at the White House's direction, he came back to Congress demanding the more extreme changes to FISA contained in the PAA without benefit of a hearing or any meaningful debate. Given the important privacy and civil liberties concerns at stake, these changes should have been better vetted prior to enactment. I welcome Director McConnell's testimony today so that we do not repeat the process by which the PAA was passed.

QUESTIONS SUBMITTED FOR THE RECORD TO THE HONORABLE J. MIKE MCCONNELL, DIRECTOR OF NATIONAL INTELLIGENCE [1]

JOHN CONYERS, JR., Michigan
CHAIRMAN

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
LINDA T. SÁNCHEZ, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
BETTY SUTTON, Ohio
LUIS V. GUTIERREZ, Illinois
BRAD SHERMAN, California
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
ARTUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota

ONE HUNDRED TENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6216

(202) 225–3951
http://www.house.gov/judiciary

LAMAR S. SMITH, Texas
RANKING MINORITY MEMBER

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
CHRIS CANNON, Utah
RIC KELLER, Florida
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio

October 9, 2007

The Honorable Michael "Mike" McConnell
Director of National Intelligence
Office of the Director of National Intelligence
Washington, DC 20511

Dear Director McConnell:

Thank you for your recent appearance before the House Committee on the Judiciary. Your testimony on FISA and the Protect America Act was insightful and will assist the Committee in its consideration of this issue as we seek to fashion enhanced legislation.

Enclosed you will find additional questions from members of the Committee to supplement the information already provided at the September 18, 2007, hearing. As you will discover in the questions, there are some sets of questions that are specifically addressed to either you or Assistant Attorney General Ken Wainstein, while other questions request answers from both you and Mr. Wainstein. You may choose whether to provide joint or separate answers to these latter questions. In addition, to the extent some questions (such as those initially contained in the September 11th letter to White House Counsel Fred Fielding) call for classified information, we are willing to make arrangements to receive the information in a manner that will protect its confidentiality.

Please deliver your written responses to the attention of Renata Strause of the House Committee on the Judiciary, 2138 Rayburn House Office Building, Washington, DC, 20515 no later than October 19, 2007. We would be pleased to accept answers on a "rolling" basis in order to expedite the process. If you have any further questions or concerns, please contact Ms. Strause at (202) 225-3951.

Sincerely,

John Conyers, Jr.
Chairman

cc: Hon. Lamar S. Smith

[1] At the time of publication, responses to questions submitted for the record to Mr. McConnell had not been received by the Committee.

QUESTIONS FOR KEN WAINSTEIN AND MICHAEL McCONNELL
APPEARANCE BEFORE THE HOUSE JUDICIARY COMMITTEE

September 18, 2007
2141 Rayburn House Office Building
11:00 a.m.

Questions from September 11, 2007 Letter to White House Counsel Fred Fielding
(Wainstein and McConnell)

1. The Committee sent a September 11, 2007 letter to White House Counsel Fred Fielding containing a list of questions concerning Administration foreign intelligence surveillance activities, which can be found on pages 4-5 of the attached letter. To date, we have yet to receive answers to these questions, which the White House has indicated should come from the relevant agencies. Please respond to those questions as soon as possible.

The Role of the FISA Court (FISC) (Wainstein and McConnell)

2. Under the PAA, the FISA Court only has the ability to determine whether the government is following its own procedures, and can stop the procedures only if they are "clearly erroneous." How can meaningful oversight occur if the court can only review procedures that it did not even initially approve under a "clearly erroneous" standard, rather than the underlying legality of the government's surveillance operations? Please explain.

3. The Fourth Amendment requires that the government get a warrant before invading a person's privacy. Explain how the PAA's procedures can be constitutional without any court review whatsoever, other than minimization?

Minimization (Wainstein and McConnell)

4. Is it correct that the "minimization" procedures that are to apply to surveillance under PAA are those specified under 50 U.S.C. sec. 1801(h)(1)-(3)? If not, which procedures apply?

5. There is much more strict minimization under section 4 of section 1801(h). That section applies to pre-PAA FISA surveillance that is undertaken without a warrant and without judicial pre-approval. Under those circumstances, minimization is very strict: no contents of an innocent American's communication can be disclosed, disseminated, used, or even kept for longer than 72 hours without a FISA court determination or an AG determination that the information indicates a threat of death or serious bodily harm. If there is to be any warrantless surveillance spying on Americans' conversations, wouldn't it be more prudent to subject it to the strict minimization procedures of 1801(h)(4), which already

apply to other surveillance without a court order, and not the more lax minimization that has previously applied only when a court did provide a court order before Americans were spied on? If not, why not.

6. Minimization procedures have been keep secret for the last 30 years. There are serious concerns as to how we can be assured that minimization procedures are effective for protecting Americans' privacy if we cannot see them. Would you support making minimization procedures public?

   a) If not, why not?

   b) Would you support producing a redacted copy?

   c) Minimization procedures only tell you what to do with US information after it is collected, therefore not revealing sources or methods. Thus, if do not support publicizing the procedures, on what do you base your objection?

7. Would you support legislation that would sequester communications to which an American is a party (and captured under this new program) that can only be used after an application to the FISA court? If not, why not?

Scope of PAA Section 105(B) (Wainstein and McConnell)

8. Does Section 105(B) permit the President to compel communications carriers to conduct domestic wiretaps so long as "a significant purpose" is to obtain foreign intelligence information concerning persons outside the United States?

9. If an individual in the United States is suspected of working in collusion with persons outside the United States – such that an investigation of one is in effect the investigation of the other – under what circumstances, generally, would you use criminal or other FISA wiretaps, and under what circumstances would you use 105(B) authority? Please explain.

10. Assuming for a moment that a member of Congress is going to meet with a high-ranking official from Syria, does Section 105(B) permit the wiretapping of that Member's office phone on the grounds that it would produce "foreign intelligence information ... concerning persons reasonably believed to be outside the United States?" Please explain.

11. Does Section 105(B) permit searching stored emails of a Member of Congress who is planning to meet with Iraqi officials? Please explain.

12. Assuming for a moment that an official at a West Coast computer company is negotiating with China to sell certain computer technology – that may or may not be sensitive, the facts are simply not certain – does Section 105(B) permit the searching of the executive's emails on the grounds that all information associated with this transaction is "foreign intelligence information ... concerning persons reasonably believed to be outside the United States"? Please explain.

13. Under Section 105(B) does the term "acquire" include "intercept"? Can the Administration "acquire" foreign relations information concerning persons overseas by "intercepting" phone conversations in the United States? Please explain.

14. Under Section 105(B) does the term "custodian" refer to anyone other than "custodians" of communications carriers?

    a) Can the President direct a "custodian" of a medical office to turn over medical records, if a "primary purpose" of the investigation is to obtain foreign intelligence information concerning someone who is overseas? Please explain.

    b) Can the President direct a "custodian" of a business, bank, or credit agency to turn over financial records to the Government, so long as a "significant purpose" of the request is to obtain foreign intelligence information? Please explain.

15. Suppose an American critic of the Iraq War travels overseas, and is thus no longer in the United States. Under Section 105(B), can the President direct "custodians" of records concerning this individual, including stored electronic communications, to produce such records to the Government with no other showing of cause that is subject to judicial review? Please explain.

Telecommunications Carriers Immunity Questions (Wainstein and McConnell)

16. 18 U.S.C. § 2511(2)(a)(ii) currently provides for telecommunications carrier immunity if one of two conditions is satisfied: a) the carrier has a court order signed by an authorizing judge; or b) the carrier has a certification from the Attorney General or another statutorily authorized official that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provisions of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. Doesn't this current statutory scheme offer the necessary protection for the telecommunications industry, advance national security interests, and provide essential oversight? If not, why not?

17. Section 2511(2)(a)(ii) certification has defined preconditions that must be satisfied, including: all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provisions of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. Blanket immunity would not have the same preconditions. Given that distinction, how can we ensure that critical checks and balances exist in the surveillance framework if blanket immunity is provided?

18. If we were to give the telecommunications carriers complete, blanket immunity, how would we guard against a total disregard of the law by companies who believe that the government simply will bail them out if they overstep legal boundaries in intercepting communications?

19. If the so-called Terrorist Surveillance Program (TSP) was perfectly legal as has been claimed, why would companies who cooperated in it need immunity?

20. The pending cases against telecommunication companies are years away from final judgment. In light of that, would it be appropriate to have the discussion of retroactive immunity wait until we determine what actions actually occurred? If not, why not?

21. Would you support something more specific than the complete amnesty you propose in your draft legislation, like simply putting a damages cap on the claims? If not, why not?

22. In discussing the controversy over the PAA with the El Paso Times, DNI McConnell said "reverse targeting" was illegal, a violation of the Fourth Amendment, and that someone engaging in such offenses "could go to jail for that sort of thing." But wouldn't the immunity provisions recommended by the administration ensure that no one would go to jail for violations of the laws governing electronic surveillance for intelligence purposes?

Scope of Authority under the PAA (Wainstein and McConnell)

23. Section 105(A) exempts surveillance "directed at" people overseas from the definition of electronic surveillance, and therefore traditional FISA court review. Because surveillance only need be "directed" at people overseas, can the government under the PAA pick up all international communications into or out of the U.S., as long as one party to the call is overseas?

24. FISA has always placed the telecommunication carriers between the government and American's private communications and records. The carriers can only turn over information in response to a specific request. Now that the government has direct access to all communication streams, how can we protect against potential abuses?

25. The Administration claims that it needs heightened access to communications because it

cannot instantaneously determine the location of each party.

a) Phone companies are capable of determining international calls versus domestic calls, and charge more for the international calls. Would it be possible for the NSA to use similar technology? If not, why not?

b) If it cannot be determined where either end of a call is, how can purely domestic to domestic communications be isolated?

c) Is it possible to institute a program by which there is initial collection of calls, none of the content is accessed until the locations of the parties are determined, and then it can be retained and only the foreign to foreign calls used?

Metadata Collection (Wainstein and McConnell)

26. On May 11, 2006, USA Today reported that "[t]he NSA has been secretly collecting the phone call records of tens of millions of Americans" and that "[i]t's the largest database ever assembled in the world." (See Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today, May 11, 2006). At any time from September 11, 2001 to the present, has the Administration, pursuant to foreign intelligence purposes, obtained call or e-mail record information or other external data on phone calls or e-mails made in the United States, through the gathering of "metadata" or otherwise, regardless of the specific title of the intelligence program or the agencies that conducted the program? Please explain.

FISA Exclusivity (Wainstein only)

27. Does the United States, through its Justice Department, agree that FISA is the law of the land, and that foreign intelligence surveillance must occur within that law? If not, why not?

28. Is the President free to disregard any provisions of FISA with which he disagrees? If so, please explain.

29. To your knowledge, since January of 2007, when the Attorney General stated that the TSP was brought within FISA, has all foreign intelligence electronic surveillance occurred consistent with FISA – both prior to and subsequent to the August amendments? Since that time have any electronic surveillance programs been conducted outside the authority of the Foreign Intelligence Surveillance Act as amended by the Protect America Act?

30. Does the Department of Justice still take the position that the Authorization for Use of Military Force (AUMF) related to the invasion of Iraq presently constitutes a basis for the President to disregard FISA? If so, please explain.

31. On December 22, 2005, the Department of Justice, in a letter to Congress, set forth the position that the President's inherent Article II powers permitted it to conduct certain terrorist surveillance outside of FISA. Is this still the Department of Justice's position?

The Federal Bureau of Investigation (Wainstein only)

32. DNI McConnell said the intelligence community is not doing massive data mining. But the FBI retains information from NSLs even where the information demonstrates the subject of the NSL was innocent. Why is this data being retained if not for data mining?

33. The Department of Justice Inspector General recently released an audit report regarding the Terrorist Screening Center, which revealed the Terrorist Screening Center watchlist had grown to over 724,000 records by April of 2007, and was increasing at a rate of 20,000 records per month. The IG found several known or suspected terrorists that were not watchlisted correctly, and a sample of records subjected to post-encounter quality assurance reviews showed 38 percent contained errors or inconsistencies. How can the intelligence community properly identify and target terrorists for electronic surveillance with such an incomplete terrorist watchlist?

Mismanagement in the Intelligence Community - - National Security Agency (McConnell only)

34. As the FISA Modernization Bill and the PAA were being debated in Congress, DNI McConnell and others in the administration suggested that advances in technology had created an "intelligence gap" which was making it more difficult for the intelligence community to keep America safe from terrorists. But according to a May 6, 2007 article in the Baltimore Sun, an internal NSA task force cited management problems as the cause of program upgrade delays, technology breakdowns and cost overruns, and called for a "fundamental change" in the way the NSA was managed. The report said NSA leadership "lacks vision and is unable to set objectives and meet them," and that NSA employees "do not trust our peers to deliver." These conclusions "are strikingly similar" to the conclusions of NSA management studies performed in 1999, yet even after 9/11 the fundamental changes recommended have not been made. Portions of this NSA task force report are not classified. Will you agree to release the unclassified portions of this report publicly and to the Committee?

35. Ensuring the proper management of intelligence would seem to be in many respects as important as increasing the authority to collect intelligence because, as the Joint

Intelligence Committee investigation into the 9/11 terrorist attacks showed, the NSA had intercepted communications linking the hijackers to terrorism long before 9/11 but that those intercepts, along with other critical pieces intelligence, were lost among the "vast streams" of data being collected. If we can assume that the NSA is collecting even more intelligence now than before 9/11, how can we be assured that the management problems at NSA are not hampering the intelligence community's ability to identify and understand which bits of intelligence are important and which are not? Please explain.

36. The September 14th Baltimore Sun report regarding a fire at an NSA "operations building" raises even more fundamental concerns about the NSA's ability to properly manage its operations. On August 6, 2007, right after the PAA was enacted, MSNBC and Newsweek reported that, "The National Security Agency is falling so far behind in upgrading its infrastructure to cope with the digital age that the agency has had problems with its electricity supply, forcing some offices to temporarily shut down." Please explain what steps are being taken in response to the reported fire and shutdown and other infrastructure and management problems.

German plot (McConnell only)

37. On September 10, you testified publicly before the Senate Homeland Security Committee that the temporary FISA changes due to the Protect America Act helped lead to the recent arrests of three Islamic militants accused of planning bomb attacks in Germany. But two days later, on September 12, you issued a contradictory statement, saying that "information contributing to the recent arrests was not collected under authorities provided by the Protect America Act." It has been publicly suggested that it was the pre-PAA FISA law, which you have criticized, that was used to help capture the terrorist plotters in Germany, and not the temporary Protect America Act.

    a) Was your statement on September 10, claiming that the temporary Protect America Act helped lead to the German arrests, actually false?

    b) Can you explain to us how it was that you came to give false information to the Senate Committee concerning the alleged contribution of the temporary Protect America Act to the German arrests?

    c) Is it true that it was the pre-PAA FISA law that was used to help capture the terrorist plotters in Germany, and not the temporary Protect America Act?

US persons "targeted" for surveillance (McConnell only)

38. In your recent interview with the El Paso Times, responding to a concern about "reverse

targeting," you stated that there are "100 or less" instances where a U.S. person has been targeted for surveillance.

a) Please explain how, when, why, and by whom it was decided to de-classify that information and reveal it publicly.

b) Over how long a period of time does that "100 or less" figure apply? For example, was it one year, five years, or since 9/11?

Declassification of Information (McConnell only)

39. At the hearing, you told Representative Scott that there is a process to declassify information and that ultimately it is the responsibility for the President to decide. Later in the hearing, you told Representative Sutton that when you did an interview you could declassify information because "it was a judgment call on your part." Could you please explain the discrepancy between your two responses to similar questions?

Concerns About the House Bill (McConnell only)

40. During the hearing, in response to my question regarding the alleged 180 degree reversal of your position on the House bill regarding FISA this summer, you claimed that you had not changed your position but that once you had actually "reviewed the words" of the House bill, you could not accept it. Please explain specifically what problems you had with the "words" of the House bill.

Previous Problems Concerning Warrantless Surveillance and Minimization (McConnell only)

41. In August 2005, the New York Times reported that John Bolton, then an official at the State Department, received summaries of intercepts that included conversations of "U.S. persons" and requested that the National Security Agency inform him who those persons were. Newsweek thereafter reported that from January 2004 to May 2005, the NSA had supplied the names of some 10,000 American citizens in this informal fashion to policy makers at many departments and law enforcement agencies. The former General Counsel at the NSA, Stewart Baker, was quoted as stating that the NSA would "typically ask why" disclosure was necessary, but "wouldn't try to second guess" the rationale.

a) What procedures are in place by entities such as the NSA that obtain summaries of conversations intercepted without a warrant to review the requests by other agencies, such as law enforcement agencies, to disclose

the identity of "U.S. persons" whose conversations are so intercepted without a warrant?

1) What showing, if any, is the requesting individual/agency required to make in order to obtain the identity of the U.S. person whose conversation was intercepted?

2) Are any such requests denied, and, if so, in the past five years, state how many such requests have been denied?

b) In the past five years, how many times have the summaries of such intercepted conversations been requested by and provided to the Office of the Vice President? To the Office of the President?

c) In the past five years, how many times have phone conversations of federally elected officials or their staff been intercepted under any surveillance program without a warrant? Do copies of those conversations still exist?

d) In the past five years, how many times have phone conversations of known members of the U.S. news media been intercepted without a warrant? Do copies of those conversations still exist?

e) In the past five years, how many times have phone conversations of attorneys in the United States been intercepted without a warrant? Do copies of those conversations still exist?

42. In 2006, Newsweek reported that the "NSA received–and fulfilled– between 3000 and 3,500 requests from other agencies to supply the names of U.S. citizens and officials ... that initially were deleted from raw intercept reports. . . . About one third of such disclosures were made to officials at the policymaking level." (See Mark Hosenball, "Spying, Giving Out U.S. Names," Newsweek, May 2, 2006).

a) During the operation of the "terrorist surveillance program," prior to its disclosure in the New York Times in December 2005, how many "U.S. names" that were masked from transcripts of intercepts were disclosed (unmasked) to government entities that requested the identities?

b) What justification was required by a requestor to obtain the identity of the U.S. person on a minimized conversation?

c) What criteria, if any, were used to determine whether a request for the identity of a U.S. person on a minimized interception was appropriate or

whether the identity of the U.S. person was necessary for a legitimate intelligence or law enforcement purpose?

d) If no justifications for identity information were required, and no criteria for review to determine the appropriateness of the request were in existence, then what purpose is served by the minimization procedures that mask a U.S. person's identity as a speaker on an intercepted phone call?

e) By name or position, which "policy makers" requested and received identity information of U.S. persons whose communications were intercepted?

43. The TSP was described in a Department of Justice (DOJ) "white paper" as "targeting the international communications into and out of the United States of persons reasonably believed to be linked to al Qaeda ...." From the date of the inception of any warrantless interception program (approximately October 2001) through the 2007 decision to bring any such program under scrutiny of FISA, was the program ever broader to encompass any other international communications in addition to those reasonably believed to be linked to al Qaeda?

44. How many U.S. persons have been arrested or detained as a result of warrantless interceptions under the surveillance programs established by the President?

45. What is the date of the first document that purports to justify the warrantless surveillance program on the AUMF? How would you respond to claims that the AUMF rationale was a creation of Administration lawyers after the December 2005 New York Times article?

46. At any time from September 11, 2001 through December 2005, did the NSA obtain "trap and trace" or "pen register" information on the phones or telecommunications equipment of U.S. persons without court orders?

a) If so, how many times?

b) If so, on what legal authority?

47. Since September 11, 2001, has law enforcement or the intelligence community conducted physical searches of the homes or businesses of U.S. citizens without warrants based on authorizations or approvals by the President or pursuant to a Presidentially authorized program?

48. Under the non-FISA warrantless interception programs, has law enforcement or the intelligence community deliberately caused the interception of purely domestic to domestic phone conversations without a FISA warrant? If so, what has been done with information so obtained?

49. Questions have been raised as to whether Christine Amanpour of CNN has ever had her telephone conversations intercepted by Administration surveillance programs. (See David Ensor, *NSA: Amanpour, Other CNN Reporters Not Targeted for Surveillance*, CNN, January 6, 2006). Has Ms. Amanpour ever been the target of warrantless surveillance – whether or not she was in the United States? Have any telephone conversations of Christine Amanpour been intercepted pursuant to any warrantless surveillance program?

Questions for Director McConnell
Submitted by Congressman Bob Goodlatte (VA-06)
Hearing on "Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II)"
September 18, 2007

In arguing for greater tools to combat terrorists, you have made statements recently in public concerning some of the significant threats the U.S. faces from foreign powers and terrorists. Specifically, in August, you stated that a significant number of Iraqis have been smuggled across the Southwest border.

1) What further information can you tell us today about those crossings? Are you aware of individuals from other state sponsors of terror that have illegally crossed the Southwest border?

2) Is securing our Southwest border a matter of national security? Do you believe that the Southwest border is sufficiently secure at this point?

JOHN CONYERS, JR., Michigan
CHAIRMAN

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
LINDA T. SÁNCHEZ, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
BETTY SUTTON, Ohio
LUIS V. GUTIERREZ, Illinois
BRAD SHERMAN, California
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
ARTUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota

ONE HUNDRED TENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6216

(202) 225–3951
http://www.house.gov/judiciary

LAMAR S. SMITH, Texas
RANKING MINORITY MEMBER

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
CHRIS CANNON, Utah
RIC KELLER, Florida
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio

September 11, 2007

Mr. Fred Fielding
Counsel to the President
Office of Counsel to the President
The White House
1600 Pennsylvania Ave., NW
Washington, DC 20530

Dear Mr. Fielding:

We are writing to follow up on the August 16, 2007 letter from the Speaker of the House and the Senate Majority Leader emphasizing the need for a prompt response to information requests by our Committee and other relevant House and Senate committees concerning Administration foreign intelligence surveillance programs, as Congress considers possible revisions to the Foreign Intelligence Surveillance Act (FISA). In particular, the Committee requests expeditious production of the documents and information on the enclosed list, which encompasses requests made to the Justice Department on January 19, February 1, May 17, and July 30, which have not produced the requested information.

To this end, we are enclosing a list of requested documents and questions. We are simultaneously submitting several additional questions to DNI Director McConnell, which relate directly to recent statements he made publicly regarding warrantless surveillance. Since the Judiciary Committee has scheduled a hearing on this issue for September 18, I would ask that you transmit as much of the information as is possible before that day. Given that many of our requests have been under review by the Administration for many months, and we were given assurances during discussion of the most recent FISA amendments that additional documentation would be forthcoming to us, this should not be burdensome or unexpected. In any event, we would ask that you set up a meeting with Judiciary Committee staff to discuss the status of any unfilled requests by no later than Thursday, September 20. This is essential given that the staff has reached out to the DNI's office, the Justice Department and to the White House over the last month to review these requests, and in each case, there has been no compliance.

We write directly to you for two reasons. First, from previous discussions with the Justice Department about our specific past requests, it is clear that it is the White House, and not the Department, that will make decisions concerning the information to be shared with Congress on this subject. Information pertinent to this request is likely to be found not just at the Justice Department, moreover, but also in offices including but not limited to the White House, Office of the Vice President, the National Security Agency, Office of the Director of National Intelligence, and the Federal Bureau of Investigation. Accordingly, we are asking the White House to facilitate responding to this document and information request across all relevant agencies.

In addition, as indicated in the August 16 letter to the President, this and similar requests from other Committees must receive the highest priority. At the Administration's urging, Congress recently enacted controversial changes to FISA in the Protect America Act of 2007, P.L. 110-55. This law, however, expires in less than six months. Our Committee has primary jurisdiction over FISA and has already begun the process of considering this issue. In the bipartisan spirit that helped produce the enactment of FISA in 1978, it is crucial that Congress and the Executive Branch cooperate and share critical information in ths area if we are to produce a law that will truly protect America's security interests while safeguarding our constitutional rights.

Indeed, throughout the process of considering this issue, we have been clear about the need for all Members of the Judiciary Committee and a sufficient number of staff to have access to information concerning the surveillance programs, including orders of the FISA court. In July, Director of National Intelligence Mike McConnell directly assured Chairman Conyers that our Members would be given access to these materials. We specifically ask that you, Director McConnell, and other key Administration officials work with us expeditiously to fulfill this pledge and to answer our requests. Moreover, as it will likely be necessary to pursue closed hearings with current or former staff from the Department of Justice, such as Jack Goldsmith or Patrick Philbin, we look forward to your cooperation on classification issues that may arise.

We appreciate that a number of our requests overlap with requests by or information already provided to other Committees, including subpoenas by the Senate Judiciary Committee. As the Speaker and Majority Leader noted, we assume there will be reciprocal disclosure of any materials that the Administration provides to the Senate Judiciary Committee. By the same token, to the extent that any of the information we request has already been provided to other Committees on a confidential basis, we would be pleased to expedite matters by obtaining access to the materials from them on a similar basis. We would similarly be pleased to work with you on other appropriate arrangements to obtain access to these materials. For example, to the extent that our requests include classified national security information, the House Permanent Select Committee on Intelligence has agreed to act as custodian for additional information provided.

We must emphasize, however, that important questions about FISA and the Administration's foreign intelligence surveillance programs remain unanswered, and we cannot fulfill our legislative and oversight functions without this critical information. We appreciate your personal attention to ensure a complete and expeditious response to each of our requests.

Responses and questions should be directed to the Judiciary Committee Office, 2138 Rayburn House Office Building, Washington, DC 20515 (tel: 202-225-3951; fax: 202-225-7680). Thank you for your cooperation in this matter.

Mr. Fred F. Fielding
Page Three
September 11, 2007

Sincerely,

John Conyers, Jr.
Chairman

Jerrold Nadler
Chairman, Subcommittee on the Constitution, Civil Rights and Civil Liberties

Robert C. "Bobby" Scott
Chairman, Subcommittee on Crime, Terrorism and Homeland Security

Enclosure

cc: Hon. Mike McConnell
Hon. Paul Clement
Hon. Lamar S. Smith
Hon. Trent Franks
Hon. J. Randy Forbes

Document and Information Request

A. Documents Requested

The Committee asks for complete and unredacted versions of the following:

1. All documents[1] from September 11, 2001 to the present constituting the President's authorization or reauthorization of any warrantless electronic surveillance[2] programs.

   This request includes, but is not limited to, the Presidential Memoranda of March 19 and April 2, 2004, and the Presidential Authorizations dated October 4, November 2, and November 30, 2001; January 9, March 14, April 18, May 21, June 24, July 30, September 10, October 15, and November 18, 2002; January 8, February 7, March 17, April 22, June 11, July 14, September 10, October 15, and

---

[1]For the purposes of this document and information request, the term"document" means any written, recorded or graphic matter of any nature whatsoever, regardless of how recorded, whether physical or electronic, whether or not maintained on any digital repository or electronic media, and whether original or copy, including, but not limited to, the following: memoranda, reports, manuals, instructions, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazine or newspaper articles, interoffice and intra-office communications, electronic mail (e-mail), any internet-enabled communication, contracts, cables, notations of any type of conversation, telephone calls, meetings or other communications, bulletins, printed matter, computer printouts, teletypes, transcripts, diaries, analyses, summaries, minutes, comparisons, messages, correspondence, press releases, circulars, reviews, opinions, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records of any kind (including without limitation, photographs, charts, graphs, voice mails, microfiche, microfilm, videotape, recordings and motion pictures), and electronic and mechanical records or representations of any kind (including without limitation, tapes, cassettes, disks, computer files, computer hard drive files, CDs, DVDs, memory sticks, and recordings) and other written, printed, typed or other graphic or recorded matter of any kind of nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.

[2]For the purposes of this document and information request, the term "electronic surveillance program" means any classified intelligence program or programs, that include electronic surveillance involving the interception of communications in the United States or when at least one party is in the United States. This includes, but is not limited to, a program that has been termed the "Terrorist Surveillance Program" (at least some portion of which the President confirmed publicly in December 2005), programs of surveillance brought under the Foreign Intelligence Surveillance Court in January 2007, the program of surveillance under the Protect America Act of 2007, P.L. 110-55, and all related, predecessor, or subsequent versions of these programs, regardless of how titled. Except as otherwise noted, "electronic surveillance" means that term prior to the definitions in the Protect America Act. For the purposes of this document and information request, the term"warrantless" electronic surveillance programs refer to such programs and activities undertaken without a warrant or order from a court.

December 9, 2003; January 14, March 11, May 5, June 23, August 9, September 14, and November 17, 2004; January 11, March 1, April 19, June 14, July 26, September 10, October 26, and December 13, 2005; and January 27, March 21, May 16, July 6, September 6, October 24, and December 8, 2006.

2. All documents from September 11, 2001 to the present, including but not limited to any legal opinions, memoranda, audits, or evaluations, concerning any programs in which, for foreign intelligence purposes, the government obtains or obtained call or e-mail record information or other external data on phone calls or e-mails made in the United States, through the gathering of "metadata" or otherwise, regardless of how the program was titled or which agencies conducted the program, including but not limited to stored communication and including but not limited to the programs referred to in the following articles: Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls,* USA TODAY, May 11, 2006; Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets,* N.Y. TIMES, September 9, 2007; and Scott Shane and David Johnston, *Mining of Data Prompted Fight Over U.S. Spying,* N.Y. TIMES, July 29, 2007.

3. All documents from September 11, 2001 to the present containing analysis or opinions from the Department of Justice, the National Security Agency, the Department of Defense, the White House, or any other entity within the Executive Branch on the legality of, or legal basis for, any warrantless electronic surveillance program, including but not limited to documents that describe why the surveillance at issue should not or could not take place consistent with the requirements and procedures of the Foreign Intelligence Surveillance Act (FISA) as they existed at the time of the document.

   This request includes, but is not limited to, any memoranda or legal opinions from the Department of Justice Office of Legal Counsel or Office of Intelligence Policy and Review, including any memoranda or opinions authored or co-authored by former Department of Justice officials Jack Goldsmith, Patrick Philbin, or John Yoo concerning legal issues related to any warrantless electronic surveillance program, and memoranda issued by the Department of Justice dated October 4 and November 2, 2001; January 9, May 17, and October 11, 2002; February 25, 2003; March 15, May 6, and July 16, 2004; and February 4, 2005.

4. All documents from September 11, 2001 to the present, including orders, memoranda decisions, or opinions of the Foreign Intelligence Surveillance Court (FISC) and Foreign Intelligence Court of Review (FISR), and pleadings submitted to the FISC and FISR, that reflect communications with the FISC or FISR or any FISC or FISR judges about warrantless or other electronic surveillance program(s), containing legal analysis, arguments, or decisions concerning the interpretation of FISA, the Fourth Amendment to the Constitution, the Authorization for the Use of Military Force enacted on September 18,2001, or the President's authority under Article II of the Constitution.

   This request includes, but is not limited to: the January 10, 2007 Orders of the FISC referenced in the January 17, 2007 letter from Attorney General Gonzales to Senator Patrick Leahy and others, bringing the warrantless electronic surveillance program "into" FISA; any Orders of the FISC that require foreign-to-foreign communications to be subject to a warrant; and any Orders of the FISC narrowing or expanding the government's ability to intercept foreign communications that may pass through equipment in the United States.

5. All documents from September 11, 2001 to the present that reflect, discuss, or describe agreements or understandings between the White House, the Department of Justice, the National Security Agency, or any other entity of the Executive Branch and

telecommunications companies, internet service providers, equipment manufacturers, or data processors regarding criminal or civil liability for assisting with or participating in warrantless electronic surveillance program(s).

This request includes, but is not limited to, any certifications by the Attorney General or other Executive Branch official pursuant to 18 U.S.C. 2511(2)(a)(ii) provided to any telecommunications company, internet service provider, equipment manufacturer, or data processor in connection with requests for assistance with warrantless electronic surveillance program(s).

6. All documents from September 11, 2001 to the present related to the classified intelligence program that was the subject of discussion during the March 2004 hospital visit to former Attorney General John Ashcroft and other events that former Deputy Attorney General James Comey described in his May 15, 2007 testimony before the Senate Judiciary Committee

   This request includes, but is not limited to:

   a) all documents from January 1, 2004 to the present related to the transfer of the powers of the Attorney General from then-Attorney General John Ashcroft to then-Deputy Attorney General James Corney in or around March, 2004 that reflect, discuss, or describe a) the date, time, or manner of that transfer of power; b) communication with or notice to White House personnel, including the President or the Vice President, about that transfer of power; c) knowledge of White House personnel about that transfer of power;

   b) any memoranda authored or co-authored by former Deputy Attorney General James Corney or any other DOJ official on or around March 10, 2004 concerning legal issues related to any warrantless electronic surveillance program;

   c) any memoranda or other documents from then-Counsel to the President Alberto Gonzales or any other White House official provided to Former Deputy Attorney General James Corney or any other DOJ official in March, 2004, concerning legal issues related to any warrantless electronic surveillance program or any proposed or actual revisions thereto; and

   d) an unredacted copy of the notes or program log of FBI Director Mueller provided to the House Judiciary Committee on August 14, 2007.

7. All documents from December 1, 2005 to the present related to the investigation by the Department of Justice's Office of Professional Responsibility (OPR) into the role of Department of Justice attorneys in the authorization and oversight of the warrantless electronic surveillance program, which was opened on January 11,2006 and closed approximately three months later after OPR investigators were denied the necessary security clearances ("OPR Investigation") that reflect, discuss, or describe the following:

   a) consideration of the request for security clearances;

   b) communications between White House personnel, including the President or the Vice President, and Department of Justice personnel about the OPR investigation or consideration of the request for security clearances; and

   c) the reasons for ending that investigation.

8. Since September 11, 2001, all audits, reports, or evaluations of or concerning any warrantless surveillance program(s), whether conducted by government employees or private companies, including any reports as to the effectiveness of minimization standards or procedures to protect U.S. persons' communications.

B. Questions

1. Since September 11, 2001, has the Administration conducted any warrantless surveillance in the United States, other than through the warrantless electronic surveillance program the President acknowledged in late 2005 (known now as the Terrorist Surveillance Program), or as explicitly authorized by FISA at the time, or any other warrantless surveillance techniques such as physical searches of home or offices or opening of mail? Are such activities continuing? Is the Administration currently conducting any foreign intelligence surveillance in the United States, other than that explicitly authorized by the Foreign Intelligence Surveillance Act (FISA)?

2. How many actionable leads have been referred to operational entities as a result of acquisitions of US persons' conversations or communications?

   a) Please break down the response as follows: 1) between September 11, 2001 and October 25, 2001; 2) between October 25, 2001 and January 10, 2007; 3) between January 10, 2007 and August 5, 2007; and 4) since August 5, 2007.

   b) Of the actionable leads referred to operational entities, what have been the results? Please differentiate between counter-terrorism, criminal investigations and prosecutions, counter-espionage, and in-theater combat operations. Please indicate with specificity whether any attacks have been averted.

3. How many conversations or communications (both incoming or outgoing) monitored under the programs have revealed a contact between a US person and someone for whom there was probable cause to believe they were in or supporting al Qaeda? How many people in the US have had email communications with someone considered to be in al Qaeda? How many of these conversations or communications have actually involved terrorist activity, as opposed to other topics of conversation? How many people have been charged with any wrongdoing as a result of such interceptions? How many terrorist activities have been disrupted as a result of such interceptions? How many people have been subjected to surveillance but not charged with any crime or otherwise detained?

4. How many persons whose conversations or communications were monitored under the programs have been subjected to any other surveillance techniques or searches, such as physical searches of home or offices, opening of mail, etc, whether subject to a warrant or not?

5. Have any US persons whose conversations or communications were monitored under the programs been detained within the United States? Have any US or foreign persons been interrogated or detained outside of the United States, whether by the United States or any other government, in significant part as a result of such monitoring?

6. Have journalists, lawyers, lawmakers (whether federal, state, or local), or aides had their conversations or communications monitored under the programs? If so, how many?

7. How many persons in the US had conversations (voice or email content) or communications (call or email data) acquired through electronic surveillance programs? In how many of these acquisitions was the person in the US the target of the acquisition? In how many of these acquisitions was the acquisition incidental, and in how many of those incidental acquisitions did the individuals subsequently become the target of acquisitions? How many warrants for continued surveillance were sought after identification of someone as a person in the US? How many such applications were denied? Please break down the response between warrantless and other electronic surveillance programs as to the following periods: a) between September 11, 2001 and October 25, 2001; b) between October 25, 2001 and January 10, 2007; c) between January 10, 2007 and August 5, 2007; and d) since August 5, 2007.

8. How many individuals have been targeted for surveillance under the Protect America Act that has involved foreign intelligence generally, as opposed to terrorism or nuclear proliferation?

9. Please identify all telecommunications companies or internet service providers that allowed the government to access communication streams in the US without warrants between September 2001 and January 10, 2007. Please identify all telecommunications companies or ISPs that have allowed access since January 10, 2007. Please break down by programs that obtained external and internal data.

10. During the time period in March 2004 in which the warrantless surveillance program did not have Attorney General certification, please identify all telecommunications companies that continued to allow surveillance without such certification. Please break down by programs that obtained external and internal data.

11. Please identify any telecommunication companies or internet service providers that refused to allow access to communication streams without court order or warrant. Please provide all letters or communications from telecommunications companies or internet service providers in which they refused to allow access to communications streams without court order or warrant. Please break down by programs that obtained external and internal data.

12. Please identify the precise legal authority that was asserted in any and all documents provided to telephone or internet service providers to obtain their cooperation between September 2001 and January 2007. Please break down by programs that obtained external and internal data. Please provide any certifications, letters, and any legal memoranda or opinions setting forth such authority.

QUESTIONS SUBMITTED FOR THE RECORD TO THE HONORABLE KENNETH WAINSTEIN, ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY, UNITED STATES DEPARTMENT OF JUSTICE [1]

JOHN CONYERS, JR., Michigan
CHAIRMAN

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
LINDA T. SÁNCHEZ, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
BETTY SUTTON, Ohio
LUIS V. GUTIERREZ, Illinois
BRAD SHERMAN, California
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
ARTUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota

ONE HUNDRED TENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6216

(202) 225–3951
http://www.house.gov/judiciary

LAMAR S. SMITH, Texas
RANKING MINORITY MEMBER

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
CHRIS CANNON, Utah
RIC KELLER, Florida
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio

October 9, 2007

Honorable Ken Wainstein
Assistant Attorney General for National Security
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Mr. Wainstein:

Thank you for your recent appearance before the House Committee on the Judiciary. Your testimony on FISA and the Protect America Act was insightful and will assist the Committee in its consideration of this issue as we seek to fashion enhanced legislation.

Enclosed you will find additional questions from members of the Committee to supplement the information already provided at the September 18, 2007, hearing. As you will discover in the questions, there are some sets of questions that are specifically addressed to either you or Director Michael McConnell, while other questions request answers from both you and Director McConnell. You may choose whether to provide joint or separate answers to these latter questions. In addition, to the extent some questions (such as those initially contained in the September 11th letter to White House Counsel Fred Fielding) call for classified information, we are willing to make arrangements to receive the information in a manner that will protect its confidentiality.

Please deliver your written responses to the attention of Renata Strause of the House Committee on the Judiciary, 2138 Rayburn House Office Building, Washington, DC, 20515 no later than October 19, 2007. We would be pleased to accept answers on a 'rolling' basis in order to expedite the process. If you have any further questions or concerns, please contact Ms. Strause at (202) 225-3951.

Sincerely,

John Conyers, Jr.
Chairman

cc: Hon. Lamar S. Smith

[1] At the time of publication, responses to questions submitted for the record to Mr. Wainstein had not been received by the Committee.

QUESTIONS FOR KEN WAINSTEIN AND MICHAEL McCONNELL
APPEARANCE BEFORE THE HOUSE JUDICIARY COMMITTEE

September 18, 2007
2141 Rayburn House Office Building
11:00 a.m.

Questions from September 11, 2007 Letter to White House Counsel Fred Fielding
(Wainstein and McConnell)

1. The Committee sent a September 11, 2007 letter to White House Counsel Fred Fielding containing a list of questions concerning Administration foreign intelligence surveillance activities, which can be found on pages 4-5 of the attached letter. To date, we have yet to receive answers to these questions, which the White House has indicated should come from the relevant agencies. Please respond to those questions as soon as possible.

The Role of the FISA Court (FISC) (Wainstein and McConnell)

2. Under the PAA, the FISA Court only has the ability to determine whether the government is following its own procedures, and can stop the procedures only if they are "clearly erroneous." How can meaningful oversight occur if the court can only review procedures that it did not even initially approve under a "clearly erroneous" standard, rather than the underlying legality of the government's surveillance operations? Please explain.

3. The Fourth Amendment requires that the government get a warrant before invading a person's privacy. Explain how the PAA's procedures can be constitutional without any court review whatsoever, other than minimization?

Minimization (Wainstein and McConnell)

4. Is it correct that the "minimization" procedures that are to apply to surveillance under PAA are those specified under 50 U.S.C. sec. 1801(h)(1)-(3)? If not, which procedures apply?

5. There is much more strict minimization under section 4 of section 1801(h). That section applies to pre-PAA FISA surveillance that is undertaken without a warrant and without judicial pre-approval. Under those circumstances, minimization is very strict: no contents of an innocent American's communication can be disclosed, disseminated, used, or even kept for longer than 72 hours without a FISA court determination or an AG determination that the information indicates a threat of death or serious bodily harm. If there is to be any warrantless surveillance spying on Americans' conversations, wouldn't it be more prudent to subject it to the strict minimization procedures of 1801(h)(4), which already

apply to other surveillance without a court order, and not the more lax minimization that has previously applied only when a court did provide a court order before Americans were spied on? If not, why not.

6. Minimization procedures have been keep secret for the last 30 years. There are serious concerns as to how we can be assured that minimization procedures are effective for protecting Americans' privacy if we cannot see them. Would you support making minimization procedures public?

   a) If not, why not?

   b) Would you support producing a redacted copy?

   c) Minimization procedures only tell you what to do with US information after it is collected, therefore not revealing sources or methods. Thus, if do not support publicizing the procedures, on what do you base your objection?

7. Would you support legislation that would sequester communications to which an American is a party (and captured under this new program) that can only be used after an application to the FISA court? If not, why not?

Scope of PAA Section 105(B) (Wainstein and McConnell)

8. Does Section 105(B) permit the President to compel communications carriers to conduct domestic wiretaps so long as "a significant purpose" is to obtain foreign intelligence information concerning persons outside the United States?

9. If an individual in the United States is suspected of working in collusion with persons outside the United States – such that an investigation of one is in effect the investigation of the other – under what circumstances, generally, would you use criminal or other FISA wiretaps, and under what circumstances would you use 105(B) authority? Please explain.

10. Assuming for a moment that a member of Congress is going to meet with a high-ranking official from Syria, does Section 105(B) permit the wiretapping of that Member's office phone on the grounds that it would produce "foreign intelligence information ... concerning persons reasonably believed to be outside the United States?" Please explain.

11. Does Section 105(B) permit searching stored emails of a Member of Congress who is planning to meet with Iraqi officials? Please explain.

12. Assuming for a moment that an official at a West Coast computer company is negotiating with China to sell certain computer technology – that may or may not be sensitive, the facts are simply not certain – does Section 105(B) permit the searching of the executive's emails on the grounds that all information associated with this transaction is "foreign intelligence information ... concerning persons reasonably believed to be outside the United States"? Please explain.

13. Under Section 105(B) does the term "acquire" include "intercept"? Can the Administration "acquire" foreign relations information concerning persons overseas by "intercepting" phone conversations in the United States? Please explain.

14. Under Section 105(B) does the term "custodian" refer to anyone other than "custodians" of communications carriers?

    a) Can the President direct a "custodian" of a medical office to turn over medical records, if a "primary purpose" of the investigation is to obtain foreign intelligence information concerning someone who is overseas? Please explain.

    b) Can the President direct a "custodian" of a business, bank, or credit agency to turn over financial records to the Government, so long as a "significant purpose" of the request is to obtain foreign intelligence information? Please explain.

15. Suppose an American critic of the Iraq War travels overseas, and is thus no longer in the United States. Under Section 105(B), can the President direct "custodians" of records concerning this individual, including stored electronic communications, to produce such records to the Government with no other showing of cause that is subject to judicial review? Please explain.

Telecommunications Carriers Immunity Questions (Wainstein and McConnell)

16. 18 U.S.C. § 2511(2)(a)(ii) currently provides for telecommunications carrier immunity if one of two conditions is satisfied: a) the carrier has a court order signed by an authorizing judge; or b) the carrier has a certification from the Attorney General or another statutorily authorized official that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provisions of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. Doesn't this current statutory scheme offer the necessary protection for the telecommunications industry, advance national security interests, and provide essential oversight? If not, why not?

17. Section 2511(2)(a)(ii) certification has defined preconditions that must be satisfied, including: all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provisions of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. Blanket immunity would not have the same preconditions. Given that distinction, how can we ensure that critical checks and balances exist in the surveillance framework if blanket immunity is provided?

18. If we were to give the telecommunications carriers complete, blanket immunity, how would we guard against a total disregard of the law by companies who believe that the government simply will bail them out if they overstep legal boundaries in intercepting communications?

19. If the so-called Terrorist Surveillance Program (TSP) was perfectly legal as has been claimed, why would companies who cooperated in it need immunity?

20. The pending cases against telecommunication companies are years away from final judgment. In light of that, would it be appropriate to have the discussion of retroactive immunity wait until we determine what actions actually occurred? If not, why not?

21. Would you support something more specific than the complete amnesty you propose in your draft legislation, like simply putting a damages cap on the claims? If not, why not?

22. In discussing the controversy over the PAA with the El Paso Times, DNI McConnell said "reverse targeting" was illegal, a violation of the Fourth Amendment, and that someone engaging in such offenses "could go to jail for that sort of thing." But wouldn't the immunity provisions recommended by the administration ensure that no one would go to jail for violations of the laws governing electronic surveillance for intelligence purposes?

Scope of Authority under the PAA (Wainstein and McConnell)

23. Section 105(A) exempts surveillance "directed at" people overseas from the definition of electronic surveillance, and therefore traditional FISA court review. Because surveillance only need be "directed" at people overseas, can the government under the PAA pick up all international communications into or out of the U.S., as long as one party to the call is overseas?

24. FISA has always placed the telecommunication carriers between the government and American's private communications and records. The carriers can only turn over information in response to a specific request. Now that the government has direct access to all communication streams, how can we protect against potential abuses?

25. The Administration claims that it needs heightened access to communications because it

cannot instantaneously determine the location of each party.

a) Phone companies are capable of determining international calls versus domestic calls, and charge more for the international calls. Would it be possible for the NSA to use similar technology? If not, why not?

b) If it cannot be determined where either end of a call is, how can purely domestic to domestic communications be isolated?

c) Is it possible to institute a program by which there is initial collection of calls, none of the content is accessed until the locations of the parties are determined, and then it can be retained and only the foreign to foreign calls used?

Metadata Collection (Wainstein and McConnell)

26. On May 11, 2006, USA Today reported that "[t]he NSA has been secretly collecting the phone call records of tens of millions of Americans" and that "[i]t's the largest database ever assembled in the world." (See Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today, May 11, 2006). At any time from September 11, 2001 to the present, has the Administration, pursuant to foreign intelligence purposes, obtained call or e-mail record information or other external data on phone calls or e-mails made in the United States, through the gathering of "metadata" or otherwise, regardless of the specific title of the intelligence program or the agencies that conducted the program? Please explain.

FISA Exclusivity (Wainstein only)

27. Does the United States, through its Justice Department, agree that FISA is the law of the land, and that foreign intelligence surveillance must occur within that law? If not, why not?

28. Is the President free to disregard any provisions of FISA with which he disagrees? If so, please explain.

29. To your knowledge, since January of 2007, when the Attorney General stated that the TSP was brought within FISA, has all foreign intelligence electronic surveillance occurred consistent with FISA – both prior to and subsequent to the August amendments? Since that time have any electronic surveillance programs been conducted outside the authority of the Foreign Intelligence Surveillance Act as amended by the Protect America Act?

30. Does the Department of Justice still take the position that the Authorization for Use of Military Force (AUMF) related to the invasion of Iraq presently constitutes a basis for the President to disregard FISA? If so, please explain.

31. On December 22, 2005, the Department of Justice, in a letter to Congress, set forth the position that the President's inherent Article II powers permitted it to conduct certain terrorist surveillance outside of FISA. Is this still the Department of Justice's position?

The Federal Bureau of Investigation (Wainstein only)

32. DNI McConnell said the intelligence community is not doing massive data mining. But the FBI retains information from NSLs even where the information demonstrates the subject of the NSL was innocent. Why is this data being retained if not for data mining?

33. The Department of Justice Inspector General recently released an audit report regarding the Terrorist Screening Center, which revealed the Terrorist Screening Center watchlist had grown to over 724,000 records by April of 2007, and was increasing at a rate of 20,000 records per month. The IG found several known or suspected terrorists that were not watchlisted correctly, and a sample of records subjected to post-encounter quality assurance reviews showed 38 percent contained errors or inconsistencies. How can the intelligence community properly identify and target terrorists for electronic surveillance with such an incomplete terrorist watchlist?

Mismanagement in the Intelligence Community - - National Security Agency (McConnell only)

34. As the FISA Modernization Bill and the PAA were being debated in Congress, DNI McConnell and others in the administration suggested that advances in technology had created an "intelligence gap" which was making it more difficult for the intelligence community to keep America safe from terrorists. But according to a May 6, 2007 article in the Baltimore Sun, an internal NSA task force cited management problems as the cause of program upgrade delays, technology breakdowns and cost overruns, and called for a "fundamental change" in the way the NSA was managed. The report said NSA leadership "lacks vision and is unable to set objectives and meet them," and that NSA employees "do not trust our peers to deliver." These conclusions "are strikingly similar" to the conclusions of NSA management studies performed in 1999, yet even after 9/11 the fundamental changes recommended have not been made. Portions of this NSA task force report are not classified. Will you agree to release the unclassified portions of this report publicly and to the Committee?

35. Ensuring the proper management of intelligence would seem to be in many respects as important as increasing the authority to collect intelligence because, as the Joint

Intelligence Committee investigation into the 9/11 terrorist attacks showed, the NSA had intercepted communications linking the hijackers to terrorism long before 9/11 but that those intercepts, along with other critical pieces intelligence, were lost among the "vast streams" of data being collected. If we can assume that the NSA is collecting even more intelligence now than before 9/11, how can we be assured that the management problems at NSA are not hampering the intelligence community's ability to identify and understand which bits of intelligence are important and which are not? Please explain.

36. The September 14th Baltimore Sun report regarding a fire at an NSA "operations building" raises even more fundamental concerns about the NSA's ability to properly manage its operations. On August 6, 2007, right after the PAA was enacted, MSNBC and Newsweek reported that, "The National Security Agency is falling so far behind in upgrading its infrastructure to cope with the digital age that the agency has had problems with its electricity supply, forcing some offices to temporarily shut down." Please explain what steps are being taken in response to the reported fire and shutdown and other infrastructure and management problems.

German plot (McConnell only)

37. On September 10, you testified publicly before the Senate Homeland Security Committee that the temporary FISA changes due to the Protect America Act helped lead to the recent arrests of three Islamic militants accused of planning bomb attacks in Germany. But two days later, on September 12, you issued a contradictory statement, saying that "information contributing to the recent arrests was not collected under authorities provided by the Protect America Act." It has been publicly suggested that it was the pre-PAA FISA law, which you have criticized, that was used to help capture the terrorist plotters in Germany, and not the temporary Protect America Act.

    a) Was your statement on September 10, claiming that the temporary Protect America Act helped lead to the German arrests, actually false?

    b) Can you explain to us how it was that you came to give false information to the Senate Committee concerning the alleged contribution of the temporary Protect America Act to the German arrests?

    c) Is it true that it was the pre-PAA FISA law that was used to help capture the terrorist plotters in Germany, and not the temporary Protect America Act?

US persons "targeted" for surveillance (McConnell only)

38. In your recent interview with the El Paso Times, responding to a concern about "reverse

targeting," you stated that there are "100 or less" instances where a U.S. person has been targeted for surveillance.

a) Please explain how, when, why, and by whom it was decided to de-classify that information and reveal it publicly.

b) Over how long a period of time does that "100 or less" figure apply? For example, was it one year, five years, or since 9/11?

Declassification of Information (McConnell only)

39. At the hearing, you told Representative Scott that there is a process to declassify information and that ultimately it is the responsibility for the President to decide. Later in the hearing, you told Representative Sutton that when you did an interview you could declassify information because "it was a judgment call on your part." Could you please explain the discrepancy between your two responses to similar questions?

Concerns About the House Bill (McConnell only)

40. During the hearing, in response to my question regarding the alleged 180 degree reversal of your position on the House bill regarding FISA this summer, you claimed that you had not changed your position but that once you had actually "reviewed the words" of the House bill, you could not accept it. Please explain specifically what problems you had with the "words" of the House bill.

Previous Problems Concerning Warrantless Surveillance and Minimization (McConnell only)

41. In August 2005, the New York Times reported that John Bolton, then an official at the State Department, received summaries of intercepts that included conversations of "U.S. persons" and requested that the National Security Agency inform him who those persons were. Newsweek thereafter reported that from January 2004 to May 2005, the NSA had supplied the names of some 10,000 American citizens in this informal fashion to policy makers at many departments and law enforcement agencies. The former General Counsel at the NSA, Stewart Baker, was quoted as stating that the NSA would "typically ask why" disclosure was necessary, but "wouldn't try to second guess" the rationale.

a) What procedures are in place by entities such as the NSA that obtain summaries of conversations intercepted without a warrant to review the requests by other agencies, such as law enforcement agencies, to disclose

the identity of "U.S. persons" whose conversations are so intercepted without a warrant?

1) What showing, if any, is the requesting individual/agency required to make in order to obtain the identity of the U.S. person whose conversation was intercepted?

2) Are any such requests denied, and, if so, in the past five years, state how many such requests have been denied?

b) In the past five years, how many times have the summaries of such intercepted conversations been requested by and provided to the Office of the Vice President? To the Office of the President?

c) In the past five years, how many times have phone conversations of federally elected officials or their staff been intercepted under any surveillance program without a warrant? Do copies of those conversations still exist?

d) In the past five years, how many times have phone conversations of known members of the U.S. news media been intercepted without a warrant? Do copies of those conversations still exist?

e) In the past five years, how many times have phone conversations of attorneys in the United States been intercepted without a warrant? Do copies of those conversations still exist?

42. In 2006, Newsweek reported that the "NSA received–and fulfilled– between 3000 and 3,500 requests from other agencies to supply the names of U.S. citizens and officials ... that initially were deleted from raw intercept reports. . . . About one third of such disclosures were made to officials at the policymaking level." (See Mark Hosenball, "Spying, Giving Out U.S. Names," Newsweek, May 2, 2006).

a) During the operation of the "terrorist surveillance program," prior to its disclosure in the New York Times in December 2005, how many "U.S. names" that were masked from transcripts of intercepts were disclosed (unmasked) to government entities that requested the identities?

b) What justification was required by a requestor to obtain the identity of the U.S. person on a minimized conversation?

c) What criteria, if any, were used to determine whether a request for the identity of a U.S. person on a minimized interception was appropriate or

whether the identity of the U.S. person was necessary for a legitimate intelligence or law enforcement purpose?

d) If no justifications for identity information were required, and no criteria for review to determine the appropriateness of the request were in existence, then what purpose is served by the minimization procedures that mask a U.S. person's identity as a speaker on an intercepted phone call?

e) By name or position, which "policy makers" requested and received identity information of U.S. persons whose communications were intercepted?

43. The TSP was described in a Department of Justice (DOJ) "white paper" as "targeting the international communications into and out of the United States of persons reasonably believed to be linked to al Qaeda ...." From the date of the inception of any warrantless interception program (approximately October 2001) through the 2007 decision to bring any such program under scrutiny of FISA, was the program ever broader to encompass any other international communications in addition to those reasonably believed to be linked to al Qaeda?

44. How many U.S. persons have been arrested or detained as a result of warrantless interceptions under the surveillance programs established by the President?

45. What is the date of the first document that purports to justify the warrantless surveillance program on the AUMF? How would you respond to claims that the AUMF rationale was a creation of Administration lawyers after the December 2005 New York Times article?

46. At any time from September 11, 2001 through December 2005, did the NSA obtain "trap and trace" or "pen register" information on the phones or telecommunications equipment of U.S. persons without court orders?

a) If so, how many times?

b) If so, on what legal authority?

47. Since September 11, 2001, has law enforcement or the intelligence community conducted physical searches of the homes or businesses of U.S. citizens without warrants based on authorizations or approvals by the President or pursuant to a Presidentially authorized program?

48. Under the non-FISA warrantless interception programs, has law enforcement or the intelligence community deliberately caused the interception of purely domestic to domestic phone conversations without a FISA warrant? If so, what has been done with information so obtained?

49. Questions have been raised as to whether Christine Amanpour of CNN has ever had her telephone conversations intercepted by Administration surveillance programs. (See David Ensor, *NSA: Amanpour, Other CNN Reporters Not Targeted for Surveillance*, CNN, January 6, 2006). Has Ms. Amanpour ever been the target of warrantless surveillance – whether or not she was in the United States? Have any telephone conversations of Christine Amanpour been intercepted pursuant to any warrantless surveillance program?

Questions for Director McConnell
Submitted by Congressman Bob Goodlatte (VA-06)
Hearing on "Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II)"
September 18, 2007

In arguing for greater tools to combat terrorists, you have made statements recently in public concerning some of the significant threats the U.S. faces from foreign powers and terrorists. Specifically, in August, you stated that a significant number of Iraqis have been smuggled across the Southwest border.

1) What further information can you tell us today about those crossings? Are you aware of individuals from other state sponsors of terror that have illegally crossed the Southwest border?

2) Is securing our Southwest border a matter of national security? Do you believe that the Southwest border is sufficiently secure at this point?

JOHN CONYERS, JR., Michigan
CHAIRMAN

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
LINDA T. SÁNCHEZ, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
BETTY SUTTON, Ohio
LUIS V. GUTIERREZ, Illinois
BRAD SHERMAN, California
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
ARTUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota

ONE HUNDRED TENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6216

(202) 225–3951
http://www.house.gov/judiciary

LAMAR S. SMITH, Texas
RANKING MINORITY MEMBER

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
CHRIS CANNON, Utah
RIC KELLER, Florida
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio

September 11, 2007

Mr. Fred Fielding
Counsel to the President
Office of Counsel to the President
The White House
1600 Pennsylvania Ave., NW
Washington, DC 20530

Dear Mr. Fielding:

We are writing to follow up on the August 16, 2007 letter from the Speaker of the House and the Senate Majority Leader emphasizing the need for a prompt response to information requests by our Committee and other relevant House and Senate committees concerning Administration foreign intelligence surveillance programs, as Congress considers possible revisions to the Foreign Intelligence Surveillance Act (FISA). In particular, the Committee requests expeditious production of the documents and information on the enclosed list, which encompasses requests made to the Justice Department on January 19, February 1, May 17, and July 30, which have not produced the requested information.

To this end, we are enclosing a list of requested documents and questions. We are simultaneously submitting several additional questions to DNI Director McConnell, which relate directly to recent statements he made publicly regarding warrantless surveillance. Since the Judiciary Committee has scheduled a hearing on this issue for September 18, I would ask that you transmit as much of the information as is possible before that day. Given that many of our requests have been under review by the Administration for many months, and we were given assurances during discussion of the most recent FISA amendments that additional documentation would be forthcoming to us, this should not be burdensome or unexpected. In any event, we would ask that you set up a meeting with Judiciary Committee staff to discuss the status of any unfilled requests by no later than Thursday, September 20. This is essential given that the staff has reached out to the DNI's office, the Justice Department and to the White House over the last month to review these requests, and in each case, there has been no compliance.

We write directly to you for two reasons. First, from previous discussions with the Justice Department about our specific past requests, it is clear that it is the White House, and not the Department, that will make decisions concerning the information to be shared with Congress on this subject. Information pertinent to this request is likely to be found not just at the Justice Department, moreover, but also in offices including but not limited to the White House, Office of the Vice President, the National Security Agency, Office of the Director of National Intelligence, and the Federal Bureau of Investigation. Accordingly, we are asking the White House to facilitate responding to this document and information request across all relevant agencies.

In addition, as indicated in the August 16 letter to the President, this and similar requests from other Committees must receive the highest priority. At the Administration's urging, Congress recently enacted controversial changes to FISA in the Protect America Act of 2007, P.L. 110-55. This law, however, expires in less than six months. Our Committee has primary jurisdiction over FISA and has already begun the process of considering this issue. In the bipartisan spirit that helped produce the enactment of FISA in 1978, it is crucial that Congress and the Executive Branch cooperate and share critical information in ths area if we are to produce a law that will truly protect America's security interests while safeguarding our constitutional rights.

Indeed, throughout the process of considering this issue, we have been clear about the need for all Members of the Judiciary Committee and a sufficient number of staff to have access to information concerning the surveillance programs, including orders of the FISA court. In July, Director of National Intelligence Mike McConnell directly assured Chairman Conyers that our Members would be given access to these materials. We specifically ask that you, Director McConnell, and other key Administration officials work with us expeditiously to fulfill this pledge and to answer our requests. Moreover, as it will likely be necessary to pursue closed hearings with current or former staff from the Department of Justice, such as Jack Goldsmith or Patrick Philbin, we look forward to your cooperation on classification issues that may arise.

We appreciate that a number of our requests overlap with requests by or information already provided to other Committees, including subpoenas by the Senate Judiciary Committee. As the Speaker and Majority Leader noted, we assume there will be reciprocal disclosure of any materials that the Administration provides to the Senate Judiciary Committee. By the same token, to the extent that any of the information we request has already been provided to other Committees on a confidential basis, we would be pleased to expedite matters by obtaining access to the materials from them on a similar basis. We would similarly be pleased to work with you on other appropriate arrangements to obtain access to these materials. For example, to the extent that our requests include classified national security information, the House Permanent Select Committee on Intelligence has agreed to act as custodian for additional information provided.

We must emphasize, however, that important questions about FISA and the Administration's foreign intelligence surveillance programs remain unanswered, and we cannot fulfill our legislative and oversight functions without this critical information. We appreciate your personal attention to ensure a complete and expeditious response to each of our requests.

Responses and questions should be directed to the Judiciary Committee Office, 2138 Rayburn House Office Building, Washington, DC 20515 (tel: 202-225-3951; fax: 202-225-7680). Thank you for your cooperation in this matter.

Mr. Fred F. Fielding
Page Three
September 11, 2007

Sincerely,

John Conyers, Jr.
Chairman

Jerrold Nadler
Chairman, Subcommittee on the Constitution, Civil Rights and Civil Liberties

Robert C. "Bobby" Scott
Chairman, Subcommittee on Crime, Terrorism and Homeland Security

Enclosure

cc: Hon. Mike McConnell
Hon. Paul Clement
Hon. Lamar S. Smith
Hon. Trent Franks
Hon. J. Randy Forbes

Document and Information Request

A. Documents Requested

The Committee asks for complete and unredacted versions of the following:

1. All documents[1] from September 11, 2001 to the present constituting the President's authorization or reauthorization of any warrantless electronic surveillance[2] programs.

   This request includes, but is not limited to, the Presidential Memoranda of March 19 and April 2, 2004, and the Presidential Authorizations dated October 4, November 2, and November 30, 2001; January 9, March 14, April 18, May 21, June 24, July 30, September 10, October 15, and November 18, 2002; January 8, February 7, March 17, April 22, June 11, July 14, September 10, October 15, and

---

[1]For the purposes of this document and information request, the term"document" means any written, recorded or graphic matter of any nature whatsoever, regardless of how recorded, whether physical or electronic, whether or not maintained on any digital repository or electronic media, and whether original or copy, including, but not limited to, the following: memoranda, reports, manuals, instructions, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazine or newspaper articles, interoffice and intra-office communications, electronic mail (e-mail), any internet-enabled communication, contracts, cables, notations of any type of conversation, telephone calls, meetings or other communications, bulletins, printed matter, computer printouts, teletypes, transcripts, diaries, analyses, summaries, minutes, comparisons, messages, correspondence, press releases, circulars, reviews, opinions, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records of any kind (including without limitation, photographs, charts, graphs, voice mails, microfiche, microfilm, videotape, recordings and motion pictures), and electronic and mechanical records or representations of any kind (including without limitation, tapes, cassettes, disks, computer files, computer hard drive files, CDs, DVDs, memory sticks, and recordings) and other written, printed, typed or other graphic or recorded matter of any kind of nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.

[2]For the purposes of this document and information request, the term "electronic surveillance program" means any classified intelligence program or programs, that include electronic surveillance involving the interception of communications in the United States or when at least one party is in the United States. This includes, but is not limited to, a program that has been termed the "Terrorist Surveillance Program" (at least some portion of which the President confirmed publicly in December 2005), programs of surveillance brought under the Foreign Intelligence Surveillance Court in January 2007, the program of surveillance under the Protect America Act of 2007, P.L. 110-55, and all related, predecessor, or subsequent versions of these programs, regardless of how titled. Except as otherwise noted, "electronic surveillance" means that term prior to the definitions in the Protect America Act. For the purposes of this document and information request, the term"warrantless" electronic surveillance programs refer to such programs and activities undertaken without a warrant or order from a court.

December 9, 2003; January 14, March 11, May 5, June 23, August 9, September 14, and November 17, 2004; January 11, March 1, April 19, June 14, July 26, September 10, October 26, and December 13, 2005; and January 27, March 21, May 16, July 6, September 6, October 24, and December 8, 2006.

2. All documents from September 11, 2001 to the present, including but not limited to any legal opinions, memoranda, audits, or evaluations, concerning any programs in which, for foreign intelligence purposes, the government obtains or obtained call or e-mail record information or other external data on phone calls or e-mails made in the United States, through the gathering of "metadata" or otherwise, regardless of how the program was titled or which agencies conducted the program, including but not limited to stored communication and including but not limited to the programs referred to in the following articles: Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls,* USA TODAY, May 11, 2006; Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets,* N.Y. TIMES, September 9, 2007; and Scott Shane and David Johnston, *Mining of Data Prompted Fight Over U.S. Spying,* N.Y. TIMES, July 29, 2007.

3. All documents from September 11, 2001 to the present containing analysis or opinions from the Department of Justice, the National Security Agency, the Department of Defense, the White House, or any other entity within the Executive Branch on the legality of, or legal basis for, any warrantless electronic surveillance program, including but not limited to documents that describe why the surveillance at issue should not or could not take place consistent with the requirements and procedures of the Foreign Intelligence Surveillance Act (FISA) as they existed at the time of the document.

   This request includes, but is not limited to, any memoranda or legal opinions from the Department of Justice Office of Legal Counsel or Office of Intelligence Policy and Review, including any memoranda or opinions authored or co-authored by former Department of Justice officials Jack Goldsmith, Patrick Philbin, or John Yoo concerning legal issues related to any warrantless electronic surveillance program, and memoranda issued by the Department of Justice dated October 4 and November 2, 2001; January 9, May 17, and October 11, 2002; February 25, 2003; March 15, May 6, and July 16, 2004; and February 4, 2005.

4. All documents from September 11, 2001 to the present, including orders, memoranda decisions, or opinions of the Foreign Intelligence Surveillance Court (FISC) and Foreign Intelligence Court of Review (FISR), and pleadings submitted to the FISC and FISR, that reflect communications with the FISC or FISR or any FISC or FISR judges about warrantless or other electronic surveillance program(s), containing legal analysis, arguments, or decisions concerning the interpretation of FISA, the Fourth Amendment to the Constitution, the Authorization for the Use of Military Force enacted on September 18,2001, or the President's authority under Article II of the Constitution.

   This request includes, but is not limited to: the January 10, 2007 Orders of the FISC referenced in the January 17, 2007 letter from Attorney General Gonzales to Senator Patrick Leahy and others, bringing the warrantless electronic surveillance program "into" FISA; any Orders of the FISC that require foreign-to-foreign communications to be subject to a warrant; and any Orders of the FISC narrowing or expanding the government's ability to intercept foreign communications that may pass through equipment in the United States.

5. All documents from September 11, 2001 to the present that reflect, discuss, or describe agreements or understandings between the White House, the Department of Justice, the National Security Agency, or any other entity of the Executive Branch and

telecommunications companies, internet service providers, equipment manufacturers, or data processors regarding criminal or civil liability for assisting with or participating in warrantless electronic surveillance program(s).

This request includes, but is not limited to, any certifications by the Attorney General or other Executive Branch official pursuant to 18 U.S.C. 2511(2)(a)(ii) provided to any telecommunications company, internet service provider, equipment manufacturer, or data processor in connection with requests for assistance with warrantless electronic surveillance program(s).

6. All documents from September 11, 2001 to the present related to the classified intelligence program that was the subject of discussion during the March 2004 hospital visit to former Attorney General John Ashcroft and other events that former Deputy Attorney General James Comey described in his May 15, 2007 testimony before the Senate Judiciary Committee

   This request includes, but is not limited to:

   a) all documents from January 1, 2004 to the present related to the transfer of the powers of the Attorney General from then-Attorney General John Ashcroft to then-Deputy Attorney General James Corney in or around March, 2004 that reflect, discuss, or describe a) the date, time, or manner of that transfer of power; b) communication with or notice to White House personnel, including the President or the Vice President, about that transfer of power; c) knowledge of White House personnel about that transfer of power;

   b) any memoranda authored or co-authored by former Deputy Attorney General James Corney or any other DOJ official on or around March 10, 2004 concerning legal issues related to any warrantless electronic surveillance program;

   c) any memoranda or other documents from then-Counsel to the President Alberto Gonzales or any other White House official provided to Former Deputy Attorney General James Corney or any other DOJ official in March, 2004, concerning legal issues related to any warrantless electronic surveillance program or any proposed or actual revisions thereto; and

   d) an unredacted copy of the notes or program log of FBI Director Mueller provided to the House Judiciary Committee on August 14, 2007.

7. All documents from December 1, 2005 to the present related to the investigation by the Department of Justice's Office of Professional Responsibility (OPR) into the role of Department of Justice attorneys in the authorization and oversight of the warrantless electronic surveillance program, which was opened on January 11,2006 and closed approximately three months later after OPR investigators were denied the necessary security clearances ("OPR Investigation") that reflect, discuss, or describe the following:

   a) consideration of the request for security clearances;

   b) communications between White House personnel, including the President or the Vice President, and Department of Justice personnel about the OPR investigation or consideration of the request for security clearances; and

   c) the reasons for ending that investigation.

8. Since September 11, 2001, all audits, reports, or evaluations of or concerning any warrantless surveillance program(s), whether conducted by government employees or private companies, including any reports as to the effectiveness of minimization standards or procedures to protect U.S. persons' communications.

B. Questions

1. Since September 11, 2001, has the Administration conducted any warrantless surveillance in the United States, other than through the warrantless electronic surveillance program the President acknowledged in late 2005 (known now as the Terrorist Surveillance Program), or as explicitly authorized by FISA at the time, or any other warrantless surveillance techniques such as physical searches of home or offices or opening of mail? Are such activities continuing? Is the Administration currently conducting any foreign intelligence surveillance in the United States, other than that explicitly authorized by the Foreign Intelligence Surveillance Act (FISA)?

2. How many actionable leads have been referred to operational entities as a result of acquisitions of US persons' conversations or communications?

   a) Please break down the response as follows: 1) between September 11, 2001 and October 25, 2001; 2) between October 25, 2001 and January 10, 2007; 3) between January 10, 2007 and August 5, 2007; and 4) since August 5, 2007.

   b) Of the actionable leads referred to operational entities, what have been the results? Please differentiate between counter-terrorism, criminal investigations and prosecutions, counter-espionage, and in-theater combat operations. Please indicate with specificity whether any attacks have been averted.

3. How many conversations or communications (both incoming or outgoing) monitored under the programs have revealed a contact between a US person and someone for whom there was probable cause to believe they were in or supporting al Qaeda? How many people in the US have had email communications with someone considered to be in al Qaeda? How many of these conversations or communications have actually involved terrorist activity, as opposed to other topics of conversation? How many people have been charged with any wrongdoing as a result of such interceptions? How many terrorist activities have been disrupted as a result of such interceptions? How many people have been subjected to surveillance but not charged with any crime or otherwise detained?

4. How many persons whose conversations or communications were monitored under the programs have been subjected to any other surveillance techniques or searches, such as physical searches of home or offices, opening of mail, etc, whether subject to a warrant or not?

5. Have any US persons whose conversations or communications were monitored under the programs been detained within the United States? Have any US or foreign persons been interrogated or detained outside of the United States, whether by the United States or any other government, in significant part as a result of such monitoring?

6. Have journalists, lawyers, lawmakers (whether federal, state, or local), or aides had their conversations or communications monitored under the programs? If so, how many?

7. How many persons in the US had conversations (voice or email content) or communications (call or email data) acquired through electronic surveillance programs? In how many of these acquisitions was the person in the US the target of the acquisition? In how many of these acquisitions was the acquisition incidental, and in how many of those incidental acquisitions did the individuals subsequently become the target of acquisitions? How many warrants for continued surveillance were sought after identification of someone as a person in the US? How many such applications were denied? Please break down the response between warrantless and other electronic surveillance programs as to the following periods: a) between September 11, 2001 and October 25, 2001; b) between October 25, 2001 and January 10, 2007; c) between January 10, 2007 and August 5, 2007; and d) since August 5, 2007.

8. How many individuals have been targeted for surveillance under the Protect America Act that has involved foreign intelligence generally, as opposed to terrorism or nuclear proliferation?

9. Please identify all telecommunications companies or internet service providers that allowed the government to access communication streams in the US without warrants between September 2001 and January 10, 2007. Please identify all telecommunications companies or ISPs that have allowed access since January 10, 2007. Please break down by programs that obtained external and internal data.

10. During the time period in March 2004 in which the warrantless surveillance program did not have Attorney General certification, please identify all telecommunications companies that continued to allow surveillance without such certification. Please break down by programs that obtained external and internal data.

11. Please identify any telecommunication companies or internet service providers that refused to allow access to communication streams without court order or warrant. Please provide all letters or communications from telecommunications companies or internet service providers in which they refused to allow access to communications streams without court order or warrant. Please break down by programs that obtained external and internal data.

12. Please identify the precise legal authority that was asserted in any and all documents provided to telephone or internet service providers to obtain their cooperation between September 2001 and January 2007. Please break down by programs that obtained external and internal data. Please provide any certifications, letters, and any legal memoranda or opinions setting forth such authority.