AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

FISA HEARING

HEARING

BEFORE THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

Hearing held in Washington, DC, September 20, 2007.

Printed for the use of the Committee

U.S. GOVERNMENT PRINTING OFFICE

38–878 WASHINGTON : 2008

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

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

SILVESTRE REYES, Texas, *Chairman*

ALCEE L. HASTINGS, Florida
LEONARD L. BOSWELL, Iowa
ROBERT E. (BUD) CRAMER, Alabama
ANNA G. ESHOO, California
RUSH D. HOLT, New Jersey
C.A. DUTCH RUPPERSBERGER, Maryland
JOHN F. TIERNEY, Massachusetts
MIKE THOMPSON, California
JANICE D. SCHAKOWSKY, Illinois
JAMES R. LANGEVIN, Rhode Island
PATRICK J. MURPHY, Pennsylvania

PETER HOEKSTRA, Michigan
TERRY EVERETT, Alabama
ELTON GALLEGLY, California
HEATHER WILSON, New Mexico
MAC THORNBERRY, Texas
JOHN M. MCHUGH, New York
TODD TIAHRT, Kansas
MIKE ROGERS, Michigan
DARRELL E. ISSA, California

NANCY PELOSI, California, *Speaker, Ex Officio Member*
JOHN A. BOEHNER, Ohio, *Minority Leader, Ex Officio Member*
MICHAEL DELANEY, *Staff Director*

FISA HEARING

THURSDAY, SEPTEMBER 20, 2007

HOUSE OF REPRESENTATIVES,
PERMANENT SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The committee met, pursuant to call, at 9:15 a.m., in room 1300, Longworth House Office Building, the Honorable Silvestre Reyes (chairman of the committee) presiding.

Present: Representatives Reyes, Cramer, Eshoo, Holt, Ruppersberger, Tierney, Thompson, Schakowsky, Langevin, Murphy, Hoekstra, Gallegly, Wilson, Thornberry, Tiahrt, and Issa.

Staff Present: Michael Delaney, Staff Director; Wyndee Parker, Deputy Staff Director/General Counsel; Jeremy Bash, Chief Counsel; Mieke Eoyang, Professional Staff; Eric Greenwald, Professional Staff; Don Vieira, Professional Staff; Mark Young, Professional Staff; Kristin R. Jepson, Security Director; Stephanie Leaman, Executive Assistant; Courtney Littig, Chief Clerk; Caryn Wagner, Budget Director; Chandler Lockhart, Staff Assistant; Josh Resnick, Staff Assistant; Brandon Smith, Systems Administrator; Chris Donesa, Deputy Minority Staff Director/Chief Counsel; John W. Heath, Minority Professional Staff; James Lewis, Minority Professional Staff; and Jamal Ware, Minority Press Secretary.

The CHAIRMAN. The committee will please come to order.

Today, the Committee will receive testimony from the Director of National Intelligence, Admiral Michael McConnell, and the Assistant Attorney General for National Security, Mr. Kenneth Wainstein, who will join us shortly, concerning the Foreign Intelligence Surveillance Act and the recently enacted legislation that expanded the administration's surveillance powers, the Protect America Act, or, as commonly referred to, the PAA.

We are here today to discuss this legislation and deal with what I think is one of the most critical issues of our time: the need to balance measures intended to protect the homeland with preserving civil liberties.

So, in that respect, I want to welcome our witness, Admiral McConnell and when Mr. Wainstein gets here as well to our hearing here.

I believe that getting this right is fundamental to the proper functioning of this great democracy, and I believe that Congress must do everything that it can to give the Intelligence Community what it needs to protect America, at the same time ensuring that we do not abandon the fundamental principles of liberty that underpinned our Constitution.

For more than 200 years, we have managed to have both liberty and security, and I intend to do my part to ensure that we continue to maintain this careful balance in the years to come.

This brings me to the recent modifications to FISA that Congress passed on the eve of our August recess, legislation that I believe alters that precious balance between liberty and security in an unnecessary and perhaps even dangerous way.

I want to begin by setting the record straight about the concerns that have been raised over the expansive scope of the new law.

There has been a lot of rhetoric from the administration and some in Congress suggesting that critics of the new Act are placing the rights of foreigners and terrorists before the need to protect America. Our position shouldn't be characterized as seeking to protect the rights of foreigners, plain and simple. Our concerns are about protecting the rights of Americans, not foreigners abroad. Thus, we are concerned for the privacy of Americans who may happen to be communicating with someone abroad.

To be clear, when a doctor living in Los Angeles calls a relative living abroad, I am concerned about her rights. When a soldier serving in Iraq or Afghanistan emails home to let his family know that he made it back from his latest mission, I am concerned about his rights and the rights of his family.

But, under the new law, we have allowed the government to intercept these calls and these emails without a warrant and without any real supervision from the judicial branch. In doing so, we have unnecessarily put liberty in jeopardy by handing unchecked power to the executive branch. I say unnecessarily because there was no need to do this in this particular way. There was an alternative, but the administration chose to torpedo it.

With that, let me explain. In late July, the Director of National Intelligence came to us and identified a specific gap which he described publicly as a backlog with respect to the FISA process that he claimed had placed our country in a heightened state of danger.

At first, he said that he needed two things: number one, a way to conduct surveillance of foreign targets in a block without individual determinations of probable cause; and, two, a way to compel communications carriers to cooperate. We gave him both of those powers.

After we shared our draft legislation with him, he came back to Congress and said that he wanted three more things. We again agreed and tailored our bill to provide each of these three things. That bill, H.R. 3356, was a result of substantial and I believe at the time good-faith negotiations with Admiral McConnell.

We gave Director McConnell everything he said that he needed to protect America. But it also did something else. It also protected our Constitution.

Yet, at the final hour and without explanation, after having repeatedly assured us that the negotiations had been in good faith, the administration rejected that proposal. Director McConnell not only rejected it, he issued a statement urging Congress to vote it down, claiming it would not allow him to carry out his responsibility to protect our Nation.

Director McConnell, today, in your testimony, I would like to hear your side of this story.

I want to hear why it is that even though we tailored legislation to meet your requirements you still rejected it.

I want to hear why you believe that H.R. 3356 would not have allowed you to do your job and why you issued a statement to that effect on the eve of the House vote.

I want to know what specifically you believe was lacking in H.R. 3356.

And, most importantly, Admiral McConnell, I want to know what it is about the inclusion of proper checks and balances and oversight in our bill that you found so unacceptable.

These are important questions, because Congress intends to enact new legislation as soon as possible as a replacement to the administration's bill. In early October, at the Speaker's request, this committee will mark up FISA legislation to address the needs of our Intelligence Community.

The new legislation will deal with the deep flaws in the administration's bill: the vague and confusing language that allows for warrantless physical searches of America's homes, offices, and computers; the conversion of the FISA Court into what we believe is a rubber stamp; and the insufficient protections for Americans who are having their phone calls listened to and emails read under this new authority as we speak here today.

Before closing, I want to take this opportunity to reiterate a critically important request for documentation regarding the NSA surveillance program that still remains outstanding.

As I have said before, to date, the administration refuses to share critical information about this program with Congress. More than 3 months ago, Ranking Member Hoekstra and I sent a letter to the Attorney General and the DNI requesting copies of the President's authorizations and the DOJ legal opinions. We have yet to receive this information.

Congress cannot and should not be expected to legislate on such important matters in the dark. I would hope that, Admiral McConnell, you and Mr. Wainstein, when he gets here, will help us in getting this material so that we can have a clear understanding of the issues that we are dealing with as a committee.

So I look forward to this hearing, and I want to now recognize the ranking member for any statement that he may wish to make.

Mr. HOEKSTRA. Thank you, Mr. Chairman. Good morning.

Good morning, Director McConnell, and we appreciate you being here. We also appreciate all of the work that you did back in July to make sure that we got a bill through the House and through the Senate to the President's desk that enabled us to provide the NSA, the Intelligence Community, with the flexibility, the agility and the tools that it needed to keep us safe.

You know, Republicans weren't invited to be a part of the negotiations as the Democratic bill was developed; and, you know, that was a disappointing effort. You know, most of the time, things in the Intelligence Committee, we have tried to do these things in bipartisan ways. But since we weren't part of the process, the only thing we could do was take a look at the end results. And there is no doubt that the bill that passed the House in a bipartisan basis, the bill that passed the Senate in a bipartisan basis did exactly what you had identified needed to happen: one, a bill in a

piece of legislation that could become law that would give the Intelligence Community the tools that it needed to be successful to keep America safe and provided very appropriately the kind of balance that we need to protect American civil liberties.

Today's hearing highlights the critical need for speed and agility. In intelligence collection, one of the things that we have learned is that an Intelligence Community that for so many years was designed to be one step faster than the former Soviet Union in the threat that came from the former Soviet Union was not going to be good enough to face the threat that we face from radical jihadists today. So the changes that we need and the changes that were made were designed to keep and to put the Intelligence Community in step with where technology was today and where the threat level was.

Since the President signed the bill, the Intelligence Community has succeeded in closing that intelligence gap that you identified in July. There should be no significant disagreement that the Protect America Act has improved our intelligence capabilities, made our country safer; and, regardless of the specific authorities used, the recent terrorism-related arrests in Germany and Denmark demonstrated why timely intelligence collection is so critical and why we must ensure that the professionals at our intelligence agencies continue to have the streamlined and effective tools at their disposal.

Not only did the Intelligence Community effectively take and participate in taking down these threats, we also know that these threats continue. There have been a couple of bin Laden tapes. There is a Zawahiri tape that may be out there today. We will have to wait for the Intelligence Community to validate its authenticity. There are rumors of another bin Laden tape.

But some of us were in the war zone over the weekend. We were in Afghanistan, we were in Pakistan, we were in Iraq, and we talked to the intelligence folks and our folks on the ground, and we asked them about the threat and said, hey, is there any way that we possibly miscalculated this threat, that it is overblown? And consistently the people have come back and said now this threat is real.

And one of the comments that came out that kind of sticks with me is one of our folks said, you know, we see threats all the time, we are working on threats all the time, and these are the kinds of things that I wouldn't want my parents to know about, the kinds of things that these people would like to do against the homeland.

And that is why it is important that America cannot afford to go dark and reopen the intelligence gaps under FISA.

You know, earlier this week, the committee received testimony information from the administration, other outside groups, that I hope have put to rest that the myth that the Protect America Act somehow reduces civil liberties protections for Americans. As Director McConnell and Mr. Wainstein will again, I think, will reaffirm today, the law does not permit reverse targeting of Americans or the searches of the homes and businesses of ordinary citizens that some have breathlessly contained in the bill.

The Department of Justice has made it clear that it believes it must seek a court order to target the communications of Ameri-

cans, and the committee will continue to carefully ensure that it does so.

We also learned that some of the activists, special interest groups that testified seek not to preserve the structure of FISA as we have known it but instead want to impose substantial and crippling new restrictions on our intelligence agency. If you go back and you read some of the testimony, it is clear. They do want to provide the civil liberties protections that we give to American citizens and people residing within our borders. They want to extend those rights to foreign individuals, including foreign terrorists, and that is the sum and total of what they intend to do.

With that, Mr. Chairman, I will submit my entire statement for the record and yield back the balance of my time.

The CHAIRMAN. Without objection.

[The statement of Mr. Hoekstra follows:]

Opening Statement

Of

Congressman Peter Hoekstra
Ranking Republican

Permanent Select Committee on Intelligence

Hearing on Foreign Intelligence Surveillance Act

September 20, 2007

Good morning. I want to welcome Director McConnell and Mr. Wainstein to this morning's hearing.

Today's hearing highlights the critical need for speed and agility in intelligence collection against America's adversaries, including detecting and preventing potential terrorist attacks. The Protect America Act recently was enacted to close significant and alarming intelligence gaps that had arisen because of restrictions that were causing the Foreign Intelligence Surveillance Act, or FISA, to be applied to foreign persons in foreign countries who were never intended to be covered by FISA. Our intelligence agencies were missing a significant portion of what we should have been getting to

detect potential foreign terrorists in foreign countries and to prevent potential attacks on Americans at a time of enhanced threat.

Since the President signed the bill, the Intelligence Community has succeeded in closing the intelligence gap, while also carefully ensuring appropriate protections for civil liberties and enhanced oversight. There should be no significant disagreement that the Protect America Act has improved our intelligence capabilities and made our country safer. And – regardless of the specific authorities used – the recent terrorism-related arrests in Germany and Denmark demonstrated why timely intelligence collection is so critical, and why we must ensure that the professionals at our intelligence agencies continue to have streamlined and effective tools at their disposal.

America cannot afford to "go dark" and re-open the intelligence gap for foreign targets under FISA. The authorities in the Protect America Act must be made permanent, along with liability protection for third parties who may assist the government and provisions to further streamline the FISA process.

Earlier this week, the Committee reviewed testimony and information from the Administration and from outside groups that I hope put to rest the myth that the Protect America Act somehow

reduces civil liberties protection for Americans. As Director McConnell and Mr. Wainstein will again reaffirm today, the law does not permit either "reverse targeting" of Americans, or the searches of the homes and businesses of ordinary citizens that some have breathlessly claimed is contained in the bill. The Department of Justice has made clear that it believes it must seek a court order to target the communications of Americans, and the Committee will continue to carefully ensure that it does so.

We also learned this week that what activist special interest groups seek is not to preserve the structure of FISA as we have known it, but instead to impose substantial and crippling new restrictions on our intelligence agencies. Those restrictions would hamper surveillance of potential terrorists in order to extend Fourth Amendment constitutional rights to foreigners that the Supreme Court has clearly said they are not entitled to. In fact, those groups want to give greater protections to terrorist suspects than American citizens who communicate with people suspected in criminal investigations under court-approved warrants get.

We also learned that the outside activists want to require the intelligence community to get federal judges to approve intelligence

collection for foreign targets in foreign countries, even though both the Constitution and longstanding legal precedent make clear that courts should give great deference to the Executive Branch in matters of national security.

At a time of continued significant threat from radical jihadists and other adversaries around the world, we cannot move backward. We must continue to ensure that our intelligence professionals have the full array of necessary tools at their disposal, consistent with the longstanding protections for civil liberties. I look forward to the testimony today.

The CHAIRMAN. We have been joined by Mr. Wainstein.

Mr. Wainstein, welcome to the hearing. We appreciate your participating here this morning.

Mr. WAINSTEIN. Thank you, Mr. Chairman.

The CHAIRMAN. With that——

Mr. ISSA. If I could make a brief opening statement. One minute.

The CHAIRMAN. Okay. Mr. Issa is recognized for one minute.

Mr. ISSA. I do think that something needs to be cleared up in real time.

During your opening statements, Mr. Chairman, I think unintentionally you talked about soldiers phoning or emailing home; and I think it is important to have in the record that, in fact, in World War II, in fact, in Korea and, in fact, in Vietnam, no soldier had an expectation that his phone calls or his emails, which didn't exist then, but his regular mails were not going to be potentially censored. In fact, someone only has to watch an old version of MASH to see what things looked like after they went through scrutiny on mail to find out whether or not it might divulge information from the battlefield.

So I would hope that when we go through this dialogue we not use our soldiers risking their lives and limbs as somehow a group that expects not to have communication heard. Just the opposite. I would say that our men and women in uniform are the first to say I am not worried about what you listen to or email coming from the battlefield. Just the opposite. I need to be kept safe by making sure that in fact we do secure that kind of information coming from Afghanistan and Iraq.

So I know the chairman is a soldier himself and didn't intend to misstate that, but I thought it had to be put into the record, and I yield back.

The CHAIRMAN. Well, I want to thank my colleague from California for clarifying the fact that we may be spying on our own soldiers.

The CHAIRMAN. With that, Director McConnell, you are recognized for your opening statement.

STATEMENT OF MICHAEL McCONNELL, DIRECTOR OF NATIONAL INTELLIGENCE

Director MCCONNELL. Thank you, Chairman Reyes, Ranking Member Hoekstra, members of the committee. It is a pleasure to appear before you today. I appreciate the opportunity to discuss the Protect America Act, as we refer to it as PAA, and the need for lasting modernization of the Foreign Intelligence Surveillance Act, which we refer to as FISA. I am pleased to be joined today by Assistant Attorney General Ken Wainstein of the Department of Justice, National Security Division.

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 in fact my duty to encourage changes to policy and procedures and, where needed, legislation to improve our ability to provide warning of terrorist or other attacks of the country.

On taking up this post, it became clear to me that our foreign intelligence capabilities were being degraded. I learned that collec-

tion 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 foreign intelligence.

I learned that Members of Congress in both Chambers and on both sides of the aisle had, in fact, proposed legislation to modernize FISA; and this was accomplished in 2006. In fact, a bill was passed in the House in 2006. And so the dialogue on FISA has been on going for some time. This has been a constructive dialogue, and I hope it continues in the furtherance of serving the Nation to protect our citizens.

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

As is well known to this committee, FISA is the Nation's statute for conducting electronic surveillance, a very important term, electronic surveillance. That is some of our disagreement on interpretation, and we will have more to say about that later.

The other part of the Act is for physical search for foreign intelligence purposes.

When passed in 1978, FISA was carefully crafted to balance the Nation's need for collection of foreign intelligence information with the need to provide protection for civil liberties and privacy rights of our citizens. There were abuses of civil liberties from the 1940s to the 1970s that were galvanized by the abuses of Watergate that led to this action we call FISA.

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

FISA is very complex, therein the problem. It is extremely complex. And in our dialogue today what we will examine is if you insert a word or a phrase, it has potentially unintended consequences, and that is the sum of our disagreement over not being able to examine the unintended consequences due to the press of time.

It has a number of substantial requirements, detailed applications, constant, extensive, factual information that require approval by several high-ranking officials in the executive branch before it even goes to the Court. The applications are carefully prepared, and they are subject to multiple levels of review for legal and factual sufficiency.

It is my steadfast belief that the balance struck by the Congress in 1978 was not only elegant, it was the right balance to allow my Community to conduct foreign intelligence while protecting Americans.

Why did we need the changes that the Congress passed in August? FISA's definition—and I mentioned this earlier—electronic surveillance simply did not keep pace with technology. Let me explain what I mean by this: FISA was enacted before cell phones, before email, and before the Internet was a tool used by hundreds of millions of people, to include terrorists.

When the law was passed in 1978, almost all local calls in the United States were on a wire, and almost all international calls

were in the air known as wireless. Therefore, FISA was written in 1978 to distinguish between collection on wire and collection out of the air.

Today, the situation is completely reversed. Most international communications are on a wire fiber optic cable, and local calls are in the air.

FISA was originally—FISA also originally placed a premium on the location of the collection. There was the cause of our problem. On a wire in the United States equaled a warrant requirement, even if it was against a foreign person located overseas.

Because of these changes in technology, communications intended to be excluded from FISA in 1978 were, in fact, frequently included in 2007. This had real consequences. It meant the community in a significant number of cases was required to demonstrate probable cause to a court to collect communications of a foreign intelligence target located overseas.

That is very important, and I would emphasize it: probable cause level of justification to collect against a foreign target located overseas.

Because of this, the old FISA's requirements prevented the Intelligence Community from collecting important intelligence information on current threats.

In a debate over the summer and since, I have heard individuals both inside the government and outside assert that the threats to our Nation do not justify this authority. Indeed, I have been accused of exaggerating the threat that the Nation faces. Allow me to attempt to dispel that notion.

The threats that we face are real, and they are serious. In July of this year, we released a National Intelligence Estimate, referred to as the NIE, on the terrorist threat to the homeland. The NIE is the Community's most authoritative written judgment on a particular subject. It is coordinated among all 16 agencies of the Community. The key judgements from this NIE are posted on our Web site, and I would encourage all to review the full details.

In short, the NIE's assessments stated the following: The U.S. homeland will face a persistent and evolving terrorist threat over the 3 years that is the period of the estimate. The main threats come from Islamic terrorist groups and cells and, most especially, al-Qa'ida. Al-Qa'ida continues to coordinate with regional groups such as al-Qa'ida in Iraq, across northern Africa and in other regions. Al-Qa'ida is likely to continue to focus on prominent political, economic, and infrastructure targets with the goal of producing mass casualties. I repeat for effect: with the goal of producing mass casualties.

Also, the goal is visually dramatic destruction, significant economic aftershock and fear in the U.S. population.

These terrorists are weapons proficient, they are innovative, and they are persistent. Al-Qa'ida will continue to try to acquire chemical, biological, radiological and nuclear material for attacks; and, if achieved, they will use them, given the opportunity to do so.

Global trends and technology will continue to enable even small numbers of alienated people to find and connect with one another, justify their anger, even intensify their anger and mobilize resources to attack, all without requiring a centralized terrorist orga-

nization, training camp or leader. This is the threat we face today and one that our Community is challenged to counter.

Moreover, these threats we face are not limited to terrorism. Countering the proliferation of weapons of mass destruction is also an urgent priority, and FISA is most frequently the source of information in that area.

The Protect America Act updating FISA passed by Congress and signed into law by the President on the 5th of August has already made the Nation safer. After the law was passed, we took immediate action to close critical gaps related to terrorist threats. The Act enabled us to do this because it contained the five following pillars:

It clarified the definition of electronic surveillance under FISA in that it should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States.

Second, under the Act, we are now required to submit to the FISA Court for approval the procedures we use to determine that a target of the acquisition is a person outside of 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 procedures involving foreign threats are now overseen by the courts.

The Act allows the Attorney General and the DNI to direct communication providers to cooperate with us to acquire foreign intelligence information.

The Act also provides liability protection proscriptively for private parties who assist us when we are directing with a lawful directive to collect foreign intelligence information.

And, most importantly, most importantly to this committee and certainly to me, FISA, as amended by the Protect America Act, 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 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 continue to need attention:

The reasons that I have outlined today 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 the United States.

Second, I call on Congress to act swiftly to provide retroactive liability protection to the private sector. It is important to keep in mind that the Intelligence Community often needs the assistance of the private sector to protect the Nation. We simply cannot go alone. We must provide protection to the private sector so that they can assist the Community in protecting the Nation, while adhering to their own corporate fiduciary duties.

Thirdly, in April of 2007, in a bill that we submitted to Congress, we asked for a number of streamlining provisions that would make processing FISA applications more effective and efficient. These changes would substantially improve the FISA process without affecting the important substantive requirements of the law.

Finally, we understand and fully support the requirement for the Community to obtain a court order or a warrant any time we target a target for foreign surveillance that is located inside the United States. That was true in 1978 when the law was originally passed. It is true today with the update that became law last month.

Mr. Chairman, that completes my remarks. I would be happy to answer your questions.

The CHAIRMAN. Thank you, Admiral.

[The statement of Director McConnell follows:]

House Permanent Select Committee on Intelligence

Hearing on the
Protect America Act 0f 2007

September 20, 2007

Statement for the Record

of

J. Michael McConnell

Director of National Intelligence

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

BEFORE THE
PERMANENT SELECT COMMITTEE ON INTELLIGENCE
HOUSE OF REPRESENTATIVES

September 20, 2007

Good morning Chairman Reyes, Ranking Member Hoekstra, 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 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.

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 <u>outside</u> 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 <u>not</u> 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 who the target is, and where 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 this Committee and the Senate Intelligence Committee 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 the Senate and House Judiciary Committees, 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 this Committee 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 staff members of this Committee 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 staff members of this Committee 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 this 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 this 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 this Committee and four of that Committee's staff members. Sixteen agency analysts and attorneys participated in this briefing.

On September 13, 2007, four staff members of this Committee and this 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.

The CHAIRMAN. With that, we recognize Mr. Wainstein for his opening statement.

STATEMENT OF KENNETH WAINSTEIN, ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY

Mr. WAINSTEIN. Chairman Reyes, Ranking Member Hoekstra and members of the committee, good morning and thank you very much for this opportunity to testify before you again concerning FISA modernization. I am proud to be here to represent the Department of Justice, and I am happy to discuss this important issue with you.

The Protect America Act is an important law that has allowed the Intelligence Community to close intelligence gaps caused by FISA's outdated provisions, and it has already made a difference. It has already made the Nation safer.

In my statement, I will briefly explain why I think Congress should make the Protect America Act permanent and also enact other important reforms to the FISA statute.

Before I do that, I would like to thank this committee for having me in closed session last week; and in particular I would like to thank you, Chairman Reyes, for proposing that we send you a letter laying out our position on some of the concerns that you and other members of the committee had with certain parts of the Protect America Act, concerns that certain language might permit the government to conduct intelligence activities well beyond those Congress contemplated before they passed the statute.

As the committee is aware, we sent that letter to you last Friday and we laid out why it is we don't think those concerns were going to become a reality in practice. I appreciated the opportunity to engage in that dialogue with you and your colleagues, and I look forward to continuing it here today.

I believe that this process will help to reassure Congress and the American people that the Act you passed in August is a measured and sound approach to a critically important issue facing our Nation.

Let me turn briefly now to why I believe that Act should be made permanent.

As I explained in my prior testimony, in 1978, Congress designed a judicial review process that applied primarily to surveillance activities within the United States, where privacy to interests are the most pronounced, and not overseas surveillance against foreign targets, where privacy to interests are minimal or nonexistent. They did this very much intentionally as they were working against a constitutional background articulated in case law and legislation that did not extend fourth amendment protections to foreigners overseas and that left the conduct of foreign intelligence surveillance against foreigners overseas within the ambit and authority of the executive branch.

With this historical background in mind, Congress created a dichotomy in the statute, a dichotomy between domestic surveillance that is governed by FISA and that is therefore subject to FISA Court review and approval and overseas surveillance against foreign targets that is not.

Congress established this dichotomy by distinguishing between wire communications, which included most of the local and domestic traffic in 1978 and which were largely brought within the scope of the statute and radio communications which included most of the transoceanic traffic at the time and were largely left outside the scope of the statute.

As a result of the revolution in telecommunications technology over the last 29 years, much of the international communications traffic is now conducted over fiber optic cables which qualify as wire communications under the statute. As a result, many of the surveillances directed at persons overseas which were not intended to fall within FISA became subject to FISA, requiring us to seek court authorization before initiating surveillance and effectively conferring quasi-constitutional protections on terrorist suspects overseas. This process impaired our surveillance efforts and diverted resources that were better spent protecting the privacy interests of Americans here in America.

As the committee is aware, the administration submitted to Congress a comprehensive proposal in April that would remedy this problem and provide a number of other changes to the FISA statute. While Congress has yet to act on that complete package, your passage of the Protect America Act was a very important step in the right direction. It amended FISA to exclude from its scope those surveillances directed at persons outside the U.S., and this has allowed the Intelligence Community to close critical intelligence gaps that were caused by the outdated provisions of FISA, and it has already made our Nation safer.

But the legislation is expected to expire in just a little over 4 months, and we urge Congress to make the Act permanent and to enact the other important reforms contained in our comprehensive proposal. It is especially imperative that Congress provide liability protection to companies that allegedly assisted the Nation with surveillance activities in the wake of the September 11th attacks.

I also wanted to assure the committee that we recognize that we must use the authority provided by Congress not only effectively but also responsibly, and I think our actions since Congress passed the Protect America Act demonstrate our full commitment to doing just that.

As we explained in the letter we sent to the committee on September 5th, we have already established a strong regime of oversight for this authority, which includes regular internal agency audits as well as on-site reviews by a team of folks from the ODNI as well as the Department of Justice. This team has already completed its first two compliance reviews, and it will complete further audits at least once every 30 days during the renewal period of the statute to ensure complete and full compliance with the implementation procedures.

In that same letter we sent to you, we also committed to providing Congress with comprehensive reports about our implementation of this authority, reporting that goes well beyond that that is required in the statute. We have offered to brief you and your staffs fully on the results of our compliance reviews. We will provide you copies of the written reports of those reviews, and we will

give you updated briefings every month on compliance matters and on implementation of this statute in general.

We are confident that this regime of oversight and congressional reporting will establish a solid track record for our use of this authority, and it will demonstrate to you that you made absolutely the right decision when you passed the Protect America Act last month.

The committee is wise to hold this hearing and to explore the various legislative options and their implications for American 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 critical importance of modernizing the FISA statute on a permanent basis.

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

The CHAIRMAN. Thank you for your testimony, Mr. Wainstein.

[The statement of Mr. Wainstein follows:]

STATEMENT OF

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

BEFORE THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

PRESENTED

SEPTEMBER 20, 2007

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

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

BEFORE THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

SEPTEMBER 20, 2007

Chairman Reyes, Ranking Member Hoekstra, 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 to close existing gaps in our foreign intelligence collection that were 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.

We already have completed two compliance reviews and are prepared to brief you on those reviews 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 this Committee during the September 6, 2007, hearing, we sent a letter to the Committee that clearly outlines the position of the Executive Branch on several such issues. 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. As I explained at a hearing of the House Judiciary Committee on September 18, 2007, the Act 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." I reiterated this conclusion at the House Judiciary Committee hearing on September 18, 2007—the statute simply 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. I reiterated this position at the House Judiciary Committee hearing on September 18, 2007. 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.

The CHAIRMAN. Mr. Wainstein, I understand you had a hard time getting in the building, so we apologize for that.

But the only thing that you missed, which is the most germane, is that we seek yours and the DNI's help in getting us the documents that the ranking member and I have requested for a number of months and are critical for our committee to understand the thinking and the process that has gone into the surveillance program, terrorist surveillance program. So if you could help, we appreciate that very much.

I don't think anyone disputes that the threats are real. I think everybody knows and understands the threats to our country are real. The issue is whether we carefully balance our ability to remain safe as a Nation while at the same time protecting our individual rights as citizens under the Constitution.

And the first question I have for you, Director McConnell, is you have told us the things that you need to improve your capabilities under FISA. Initially—and we are going back to the three things you identified previously—no individual warrants for targets abroad, a way to compel telecommunications companies to cooperate, and individual court orders from targeting an American.

I believe that H.R. 3356 gave you all of those elements. When we discussed these issues with you last month, you told us then that the bill was acceptable and then only to find out later that it was rejected.

So the first question I have is, do you still think that H.R. 3356 doesn't offer you the things that you need by way of these three requirements? And if it doesn't, which ones does it not offer or which ones do we fall short on?

Director MCCONNELL. Thank you, Mr. Chairman. I appreciate the question and an opportunity to explain in context, if I could.

In the course of this dialogue, which intensified pretty briskly toward the end of July, we exchanged between us seven different drafts. While I am, one, not a lawyer, two, imposed on the lawyer team that I had—I had more than 20—that we wanted and needed these three main points that we are trying to achieve: no warrant for overseas, as you mentioned, getting help from the private sector, and requiring—and this is one of my major points, is I thought the 1978 law was right requiring us to get a warrant if it involved U.S. persons. That was sort of my philosophical underpinning.

What happened is the law is very, very long and extremely complex, so if someone has an issue with a part of it and they want to change a phrase or attack a part of it in the language as entered, we don't know the impact of that until we can sit down, examine it and so on. I have a team of 20 lawyers that are experts in every aspect of that.

Let me give you a couple of examples: There are claims and worries about reverse targeting. What does that mean? The assertion is the government wants to know about a U.S. person in the country. Therefore, we would target someone overseas that might contact that person because we wouldn't have to have a warrant to target the person overseas. So language was included to address reverse targeting.

Now what that does is introduce ambiguity and uncertainty. You don't know, we don't know how the Court would interpret such language once it gets there. You build a level of uncertainty.

Also, reverse targeting is unlawful. So, my view, it wouldn't be required to be inserted in the law, and I was very worried about the uncertainty. So it was just not required.

That is one example, and there are a number of examples.

Let me move to minimization, words in the draft to address minimization, and what do I mean by "minimization?" When we are conducting surveillance against a foreign target and a foreign target called into the United States, we have to make some decision with regard to that transaction. It has been true for 30 years. It is true on the criminal side. It is an artifact of doing this business.

Minimization has been examined by the Court. It has been found to be reasonable by the Court. So in the case that a foreign terrorist was calling in the United States, if it were incidental and innocent, it would be purged from our database. If it were real, that might be the most important call that we intercepted. And so one would ask, well, what would you do with that? In that case, once the sleeper or someone in the country became a target of interest for probable cause, we would get a warrant.

So, in my view, minimization for 30 years or almost 30 years has worked well; and if you attempt to adjust it, you don't fully understand or appreciate the outcome.

And there were a few other things. I will just give you some, not to take too much time.

There was information about the definition of electronic surveillance. There are four different definitions, and what we had proposed is changing the definition so it excluded a foreigner in a foreign country. The draft you had still included definitions of electronic surveillance to include foreign persons. So you are back in a situation of not knowing how the Court would interpret it.

So my problem was, one, limited time to review, get the draft, short turnaround, sit down with the lawyers; and we are coordinating between all of the experts and would say, look, we don't know what this means. So I was put in a position where I could do nothing but say can't support it because we haven't had a chance to examine it.

That is the sum and substance of what happened.

The CHAIRMAN. Thank you, Director McConnell.

I am a bit perplexed, because you are talking about a lot of things that were not included in 3356. The negotiations that we had with you covered those three points that you said you needed.

Director MCCONNELL. Yes, sir. They did.

The CHAIRMAN. And they expanded the legislation on the second go-round to include all foreign intelligence. If you remember that issue, which you made a case for making sure that, all foreign intelligence should be part of that process.

But getting back to my original question, did 3356 give you the three things that you said you needed that we were negotiating?

Director MCCONNELL. No, sir. The thing that I was worried about most was no warrant against a foreign target, foreign country. Because the wording in 3356, the definition left it uncertain. So you still would have the Court involved, and so our problem was

how would the Court interpret it. So it would put us back in the untenable situation.

Let me go back to the end of July, first couple of days of August.

The CHAIRMAN. But, Director McConnell, then why would you tell us at the time that we were having this discussion that it did everything that you wanted?

Director MCCONNELL. I said if it addressed the three fundamental—remember, I am not the lawyer. I am the operator saying you have got to have these three things.

When you examine the words, I wasn't assured that I had the three things.

And the reason I want to go back to the end of July and the first part of August, the Congress had a timetable that was driving the schedule. We exchanged seven drafts. Each turn—and, remember, I am doing this on the Senate side, also. Each turn we were given very limited time to actually examine the draft. And when I say 20 lawyers, I don't just imagine 20 lawyers sitting around a table. These are experts in aspects of this because it is so complex.

So we would have to have time to say, if you changed a phrase, just the modification to electronic surveillance, what does that mean in the ultimate interpretation? And that was the problem that we faced. I could not, with certainty, believe that the very first thing I asked for, the fundamental premise going in, which was the reason FISA was created, no fourth amendment protection for foreigners that are suspected of activity that is inimicable to the interests of the United States. There is no intent to do that. But 3356 could still get you there.

Now it is an interpretation, but because we didn't have time to sit down and have dialogue on a give and take, that is why we were—I said I can't support it. I just—I don't have confidence it would come out the way you intended it.

The CHAIRMAN. I will leave that for a couple of other members to pursue further.

I want to move on—in the interest of time—and ask you to switch topics and ask you, in your testimony before the House Judiciary Committee on Tuesday, you made the statement that no American had been targeted with electronic surveillance without a warrant. But if you recall in your interview in the El Paso Times last month, you said the number of Americans was a hundred or fewer. I believe that there has been a lot of confusion on this one issue. So I would like to try to clarify that discrepancy.

Can you tell us, Mr. Director, since September the 11th, 2001, how many Americans have been targeted with electronic surveillance without a warrant?

Director MCCONNELL. I can't tell you the answer to that because I don't know. I was asked the question earlier in the week in the committee, and then I clarified my answer when I thought maybe I left a misimpression. I can only talk about the period of time since I have served. The other part is hearsay, and I could probably go find it out, but I don't know.

What I was attempting to do and what I have learned by this process is that no good deed goes unpunished. What I was attempting to do at a summary level was to provide some factual informa-

tion that people could deal with understanding the magnitude of this issue.

There were many, many claims about the Intelligence Community conducting massive surveillance against the American public, a drift net over the entire country looking at every issue and transaction and doing data mining.

What I was attempting to give perspective to is there are thousands of foreign intelligence targets and in the course of these thousands of operations we are conducting against foreign intelligence targets on occasion a foreign terrorist called in the United States. Now, when a foreign terrorist called in the United States and now there is reason to believe that there is something to do with terrorism, then we would be required to get a warrant.

So in this specific instance starting in the January-February time frame, given the numbers we were dealing with where it would result in some surveillance of a U.S. person for which we got a warrant, that number was about a hundred or less. That was the point of what I was attempting to do at a summary level, provide the Congress, because you were being discussed in the press and a lot of criticism about what we did pass or what you all passed and the President signed, so all my intent was to do was to provide some context so people had a better way to understand this and appreciate it.

So don't know about 2001, wasn't here. I could go try to find out. But, on my watch, none without a warrant and about a hundred where we got a warrant and we had reason to believe where we needed one.

The CHAIRMAN. I think that is part of what led to the confusion on this issue, because you said zero to the Judiciary Committee.

Director MCCONNELL. The question was without a warrant, zero without a warrant. So once—remember, a terrorist calls in, now we have reason, we get the warrant, so zero without a warrant, a hundred with a warrant. That was what I was trying to explain.

The CHAIRMAN. Is there anybody accompanying you today that you can consult with so you can give us an idea of the number of Americans since September the 11th that have been targeted with electronic surveillance?

Director MCCONNELL. Let me ask and find out.

I can't give you a number, sir. I can possibly provide you with one at a classified level.

I used to serve as Director of NSA years ago. When you are collecting information, the task for in the collection process is processing out information. You could have data in a database that—you don't know what is in the database. It hasn't been examined. Remember, we are talking billions of things going on.

So the way the process is designed is, at a point in time, the database, it just shorts ground, goes off, you don't hold it anymore.

The situation would be, given now that you have had data and you have some reason to examine the data, if there was incidental collection against a U.S. person in the data, has nothing to do with any foreign intelligence reason, now you know it you have to destroy it. Get it out of your database. If it had foreign intelligence value, terrorism, whatever, now you must report it.

Now, let us say it was a U.S. person inside the United States. Now that would stimulate the system to get a warrant. And that is how the process would work.

Now, if you have foreign intelligence data, you publish it. Because it has foreign intelligence value and somebody wants the identity. There is a very structured process that you would have to go through to get approval to be aware of what that person's identity might be.

So it is something that is the workforce of thousands of people are trained in. It is something they review on a yearly basis. It is something that is very structured to prevent any potential abuse or any claims of spying on Americans.

The CHAIRMAN. But is it your position that you can go back and give us the information, again, since 9/11?

Director MCCONNELL. What I am highlighting for you is it will be probably a range. One I am pretty sure——

The CHAIRMAN. The best that you can do under those circumstances.

Director MCCONNELL. It would probably be a classified answer.

The CHAIRMAN. We appreciate that.

The last thing, and I will turn it over to the ranking member for his questions, is when will you furnish us the documents that we have requested?

Director MCCONNELL. Sir, my understanding is there is a negotiation going on between the Judiciary Committees and the White House with regard to that documentation. I am generally aware, I have made my recommendations known, and so that is a process that is ongoing now. I don't know specifically where it is in the decision cycle. Maybe Mr. Wainstein, he might have some additional insight.

Mr. WAINSTEIN. No, sir. I am afraid I actually don't have any sort of updating information as to where those negotiations are. I know they are ongoing between various parts of the administration and various committees up on the Hill. But I really couldn't tell you what the status is at this point.

The CHAIRMAN. Any assistance both of you gentlemen can give us we would appreciate it.

With that, I will recognize the ranking member for his questions.

Mr. HOEKSTRA. Thank you, Mr. Chairman.

Admiral McConnell, can you explain how the FISA structure has accounted for the possibility that the communications of Americans may be intercepted when targeting foreign persons? I mean, the law has been around since 1978. This is not a new problem, correct?

Director MCCONNELL. That is correct.

Mr. HOEKSTRA. So how have the folks at NSA dealt with this since 1978? How would this have been managed under the period of time that—in the Clinton administration when you were running NSA? What are the processes and the procedures that go through this talk about collection of Americans?

Director MCCONNELL. First of all, it is unlawful to collect against U.S. persons without a warrant. So that is where you start.

Second——

Mr. HOEKSTRA. Since 1978, if you are targeting and collecting against an American, the people at NSA have gone through the rigorous training; and that has always been subject to congressional oversight, that you have got to get a warrant?

Director MCCONNELL. That is correct. And, sir, I would even submit that I think we could have been better in the 9/11 situation had we perhaps thought about it differently. We put so much emphasis, the Community was trained and drilled and rehearsed and had such a cultural affinity with what we just described that any time it had anything to do with United States, it was—we just didn't do it.

So if Osama bin Laden himself was being tracked in Pakistan or Turkey or Europe or wherever, the minute he comes into the United States, he is now a U.S. person, and it is a different situation.

So the process—and when you are—first of all, the Community is tasked and responsible for only doing one thing, collecting foreign intelligence information. So when you are doing your foreign intelligence collection mission, there are circumstances whereby a foreigner could call into the United States. And we refer to that as incidental. When an incidental situation like that develops, the rules are it must be minimized. Once recognized and minimized, it is incidental. It must be purged from the database. That is what we have done for almost 30 years.

If it turns out that it has intelligence value for whatever purpose—terrorism, crime, whatever—you are required to report it. Even in the report you are required to protect the identity of the U.S. person.

So that is the way the processes work. It is called minimization. It is something that has been examined by the Court, endorsed by the Court, and it actually originated on the criminal side where criminal investigators would have a warrant to, for example, conduct surveillance against a specific person in the Mafia. That person may have incidental phone calls and nothing to do with the crime or breaking the law. That was called a minimization process. That is where it came from. That is how it has been used in the community.

Mr. HOEKSTRA. Those protections are still in place?

Director MCCONNELL. Yes, sir they are.

Mr. HOEKSTRA. You stated in the Judiciary Committee that you were required earlier this year to—or that you were required to get a FISA order to conduct surveillance on Iraqi insurgents who had captured Americans. Can you discuss that case any further?

Director MCCONNELL. I have to be a little careful because of sources and methods issues.

But the situation was, as you know, because global communications move on wire, you can have a situation where information would pass on a wire through this country. And so for us to specifically target individuals that were involved in that kidnap, we had to go through a court order process.

Now when we talked about this before, people frequently say, well, wait a minute. Why don't you just do emergency FISA? Well, that is the point. We are extending fourth amendment rights to a terrorist foreigner, in a foreign country who has captured U.S. sol-

diers, and we are now going through a process to produce probable cause that we would have authority to go after these terrorists.

So then people will say, why don't you just—you have got emergency authorization. Well, emergency authorization doesn't mean you don't go through the process, which is probable cause. So some analyst has just got to do it, and some official has got to sign it out, and it has got to come to either me or some other officials, and it goes to the Attorney General and then to the FISA Court.

So even though you could go faster, some would assert or just automate the process and you go the speed of light. The human brain still has to engage, and you still have to certify the accuracy.

So the reason I raise the case is it is my fundamental belief that that foreigner in a foreign country, known terrorist, has no right to protection of the Fourth Amendment. And the process slowed us down. That was what I was complaining about.

Mr. HOEKSTRA. And the situation was one where we ought to be clear about, these were Americans that were captured?

Director MCCONNELL. Yes, sir.

Mr. HOEKSTRA. And the way that the process required you, required you to go through a court process to get a FISA order to be able to listen.

Director MCCONNELL. And the reason, sir, is two things: the mode of communications that was used and where it was intercepted. That was the only issue.

Now let us go back to the terrorists in Baghdad. If they had had a push-to-talk phone or if they had a cell phone talking to a tower or if they used signal flags or if they had talked to a cell phone to a satellite, any of that, there is no warrant because it is in the air and it is in a foreign country.

But because they used a mode of communication that involved wire and the wire passed the United States, that was where the technology did not keep pace—where the law did not keep pace with technology. It was because of how and where that put us in that situation. They were using a device or devices that caused us to stop and get a warrant, so it slowed us down.

Mr. HOEKSTRA. Thank you.

With that, Mr. Chairman, I will yield back the balance of my time.

The CHAIRMAN. I thank the ranking member.

Just to be clear on this particular case that you mentioned, the emergency provisions—and we have had testimony to this effect—kick in so you can start monitoring immediately and then you evaluate whether or not within those 72 hours you are going to need to take it to the FISA Court?

Director MCCONNELL. I didn't make myself clear. I am sorry. I am failing here.

Here is my point: Emergency provisions still have to meet a probable cause standard. So I can have emergency provisions. I still have to go through the process of probable cause, get people to certify and take it to a court. My argument is that a foreigner in a foreign country shouldn't be worried about emergency process or probable cause. If it is a foreigner in a foreign country, that is our mission. We should be doing that without involving a court. That is the point I am trying to make.

The CHAIRMAN. I just wanted to make sure that we were clear so that the American people don't misunderstand that everything wasn't done as quickly as possible.

Director MCCONNELL. Could we have gone faster? No question. I am sure we could have gone faster on the edges. I want to make sure the American people clearly understand this. Going fast does not take away the fact it still has to meet a court standard.

So the issue is we are meeting a probable cause standard that still has to be reviewed by a court, and my argument is that is the wrong way to do this, but we shouldn't even be going down that path.

Mr. WAINSTEIN. May I piggyback on that for a quick second?

I think that is a very important point. Because people hear that we have this emergency authority and assume that, okay, we can sort of go up on it without any process at all.

Keep in mind that under FISA, under the emergency provisions of FISA, the Attorney General of the United States, and now with recent amendments to the statute delegated down to me, we have to find that there is probable cause that the person we want to surveil overseas is an agent of a foreign power. And if we don't find that, we are not allowed under the statute to go ahead and authorize emergency authority and within 72 hours we have to make that showing to the satisfaction of the FISA Court.

So it is a very important responsibility. It is nothing we take lightly.

As a result, analysts, whoever else is involved in the process, they have to pull together the information to establish that, to make that showing, and that is not—that can take some time in order to get that evidence together.

And keep in mind that, were it not for that, if these surveillances overseas did not fall within FISA, we would not have to make a showing that the person that we want to surveil is connected to any particular foreign power which is—you know, that is our foreign intelligence. I mean, our foreign signal intelligence surveillances don't require that, and they shouldn't for surveillances outside the United States, they shouldn't fall within FISA.

It is very important that people should understand the fact that we have emergency authority doesn't mean we can automatically snap our fingers.

Director MCCONNELL. That is why my number one point from the day I came back into active duty and looked at it as my number one point was, since I was on active duty before, I never had to have a warrant for a foreign target in a foreign country and now all of a sudden I had to. That was the main thing I was trying to get people to recognize and deal with.

The CHAIRMAN. Ms. Eshoo.

Ms. ESHOO. Thank you for holding this public hearing, Mr. Chairman. I think it is so important, because the American people are really worried about this. All one has to do is look at the editorials that were carried in newspapers in different parts of the country and the stated concerns about the bill that was passed.

Mr. Director, I want to ask you about a specific interview that was carried—the chairman mentioned it—in the El Paso Times

that ran on August 27th. You revealed a great deal of information that had previously been considered classified.

I remember the discussion and the number being given to committee members and I don't know whether the word "warning" was there, but it was certainly reinforced that this was a highly classified number.

So, for example, you discussed the mechanics of the FISA applications and court review, including the recent changes in FISA case law that necessitated warrants for wire communications traversing our country. You also confirmed that private sector companies assisted in conducting the President's warrantless surveillance program.

Now my question on this is, did you discuss with the White House your intent to declassify these facts in advance of the interview?

Director MCCONNELL. No, I did not.

Ms. Eshoo. If not, why not?

Director MCCONNELL. The control of classified information is subject to Presidential authority, and the President delegates that authority to me, and it becomes a judgment call.

Ms. ESHOO. So simply by stating in that interview with the El Paso Times the information just automatically became declassified because you stated it publicly?

Director MCCONNELL. It becomes a judgment call. I will repeat some of the remarks I made earlier with regard to why I chose to do that. There were many claims and counterclaims.

You opened your comments, saying, "Americans are worried." Some were asserting in those same editorials that my community was conducting a drift net of surveillance.

Ms. ESHOO. I don't want to go back to what you have said before. I appreciate your wanting to say more that was stated earlier today, but I only have a limited amount of time.

I was really stunned when I read that, I have to tell you. I think others were as well.

Does the same thing occur if we as members of the committee state a classified number and we decide it should just be declassified?

Director MCCONNELL. You would have to request authority to do that. I have that authority, and I made a judgment. It was in my judgment call.

Ms. ESHOO. Were you aware, by reviewing the involvment of private sector companies, that it undermined the Justice Department's case, their defense against the lawsuit about the President's program?

Director MCCONNELL. I am sorry. Repeat the question.

Ms. ESHOO. I mean, there was a lot of speculation. You confirmed that private sector telecommunications companies were assisting in the President's program. I am just asking you if you were aware if that undermined the Justice Department's defense against the lawsuit.

Director MCCONNELL. The words I chose were private sector. If you go back and closely examine all the articles that covered my interview, they would quote me up to a point, and then it would

stop the quotes and go on to name specific companies or telecommunications or whatever.

Ms. ESHOO. I think we may view it differently, which is legitimate.

Director MCCONNELL. I can refer you back to the article, which was printed verbatim.

Ms. ESHOO. After the Act passed, you claimed that because of the congressional and public debate over changes in FISA, "Some Americans are going to die."

Director MCCONNELL. Yes, ma'am.

Ms. ESHOO. Do you really believe that because we have a public debate in the Congress of the United States about surveillance, about the Foreign Intelligence Surveillance Act, that Americans are going to die?

Director MCCONNELL. Yes, ma'am.

Ms. ESHOO. That is a heavy statement.

Director MCCONNELL. Intelligence business is conducted in secret for a reason.

Ms. ESHOO. Did you ever advise the Congress not to debate this in public and that you believed Americans were going to die?

Director MCCONNELL. I have been very clear about this all along. This is very important for us to get this right so we can do our mission to prevent Americans from dying.

Ms. ESHOO. That is not what you said.

Director MCCONNELL. If you would allow me to finish, I will tell you what I intended to say, what I did say.

If you compromise sources and methods; and what this dialogue and debate has allowed those who wish us harm to do is to understand significantly more about how we were targeting their communication.

Ms. ESHOO. Mr. Director, with all due respect, I think that you put out classified information; and simply by stating because you are director and say that you have the ability to do that and that it just became declassified, I think that that was very important information that shouldn't have gone out. That is only my judgment.

Now, you are standing by your previous quote that when we debate these that some Americans are going to die. I think that is a stretch. I think because of these things it has done damage to what you bring forward. It puts a dent in the credibility.

And I think that there are some Members of Congress that are being affected by this. That is why I raise it.

Chairman REYES. Thank you, Ms. Eshoo.

Ms. Wilson.

Mrs. WILSON. Thank you, Mr. Chairman.

Mr. Wainstein, would the Protect America Act affect the e-mail of a soldier communicating with his family back home?

Mr. WAINSTEIN. Under certain circumstances, it would, yes. The Protect America Act allows us to target surveillance on persons overseas.

Keep in mind that one of the things that we have to do is, we have to satisfy the various elements, and one of them is, it has to have a significance for intelligence purposes. We can't target anybody for kicks. The DNI and AG have to certify that there is a foreign intelligence purpose for that surveillance.

Keep in mind also, if this is an American soldier that is a United States person, there is what is called the 2.5 process in place, 2.5 under Executive Order 12333, which says that before we can target an American overseas for surveillance, the Attorney General has to find probable cause.

Mrs. WILSON. The Attorney General would have to certify that there is probable cause to believe that that soldier overseas is an agent of a foreign power. Is that correct?

Mr. WAINSTEIN. The Attorney General would have to find that, yes.

Mrs. WILSON. Thank you.

With respect to reverse targeting, Mr. Wainstein, would the Protect America Act allow a circumstance where you really want to listen to a doctor in America, so you wiretap his relatives overseas? Would that be against the law?

Mr. WAINSTEIN. It would be.

Mrs. WILSON. Admiral, you testified before the Judiciary Committee, and it has already been discussed a little bit here. You said, "And let me give you an example: An American soldier is 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."

In that circumstance, did you try to get an emergency FISA?

Director MCCONNELL. Yes, ma'am.

Mrs. WILSON. How long did it take from the time the United States knew it had a target until you were able to get the Attorney General to sign off?

Director MCCONNELL. Ma'am, I will have to get you an exact answer. If my memory serves, somewhere in the area of 12 hours or so.

Mrs. WILSON. So it took a minimum of about 12 hours to get the probable cause, get it all the way through to get the signal to turn on the wiretap?

Director MCCONNELL. Yes, ma'am.

The point I was trying to highlight is the fact of probable cause, and the standard has to be a probable cause standard that a court would approve.

Mrs. WILSON. If that terrorist in Baghdad was using a push-to-talk phone, you could have gone up immediately?

Director MCCONNELL. That is correct. The reason was the mode of communication; that is what drove us to a warrant requirement.

Mrs. WILSON. So we had U.S. soldiers who were captured in Iraq by insurgents, and for 12 hours immediately following their attack, you weren't able to listen to their communications; is that correct?

Director MCCONNELL. That is correct.

Mrs. WILSON. If it was your kid, is that good enough?

Director MCCONNELL. The reason I try to be as straightforward and open on this subject as I have, is because it is so important that we get this right. You may even accuse me of declassifying information, a warmonger, a fearmonger or whatever, but we have got to get this right because sometimes those timelines are so tight, it could cost us American lives.

We have to not extend fourth amendment protections to a foreign terrorist, particularly in something like this where they are holding a U.S. hostage.

Mrs. WILSON. Mr. Wainstein, you are a Justice guy; you are familiar with things like the Amber Alerts and the importance of those first hours and gathering information to protect American lives, often children.

Mr. WAINSTEIN. The point is, we need to be agile, we need to be able to jump and respond to circumstances immediately.

This is a dangerous game. It is in this situation and some of the situations that happen every day, anything that slows down that process makes it more cumbersome, makes it more likely terrorists will win.

Mrs. WILSON. Thank you.

The threat persists, and you both have testified to that fact and that our laws did not, before the Protect America Act, work fast enough to protect this country against people who were trying to create mass casualties against Americans.

I thank both for your work.

I yield back.

Chairman REYES. Thank you, Ms. Wilson.

I think that is an abhorrent failure of leadership on our part, and we shouldn't be worried about whether or not we are legally compliant when American lives are at stake, especially in the combat situation.

Mrs. WILSON. Mr. Chairman, may I ask a question?

Chairman REYES. You may.

Mrs. WILSON. If they had not followed the law in that circumstance, if they had said, forget the FISA, don't worry about the Attorney General, just go up on that number and we will worry about explaining later, would that maybe break the law?

Chairman REYES. The testimony that we had in committee by Mr. Jim Baker the other day is that all it takes is a phone call explaining that American lives are at stake in a combat zone.

I think it gets back to the bureaucracy and a failure, again, to recognize that American lives are at stake. I think it is a commonsense thing to work with.

Director MCCONNELL. Sir, the point—maybe not being captured—here is, even in an emergency you still have to get approval. Someone has to say "yes." It's according to the law.

In this case, it is the Attorney General, so the process to get the data and put it in a format and move it through the system and get it approved.

Chairman REYES. There were a number of other circumstances in this particular case, but again I think it is imperative that we understand that there is that capability of making that phone call. I would be surprised if they wouldn't say, let's go up on it, let's make sure we are building a case, because all the elements were there, that American soldiers' lives were in danger.

With that, Mr. Holt, you are recognized for 5 minutes.

Mr. THOMPSON. Mr. Chairman, before you go to Mr. Holt, would you yield for a question to the Chair on the issue that we are discussing regarding these soldiers that were captured? Could we get

some clarification on why it took 12 hours? Was it a bureaucratic holdup, was it a legal holdup, or was it a technology holdup?

Given the testimony we heard from Mr. Baker yesterday, it seems ridiculous that it would take 12 hours, if we have identified a target, to be able to ascertain the information we need to protect the lives or to find the soldiers that had been captured. I think there is a lot that is not being explained here.

Chairman REYES. We do have, and the committee does have, the information, including the timeline and other circumstances that were involved, including that the Attorney General was out of town and issues like that.

Again, it is available for any member of the committee. We do have it.

Mr. WAINSTEIN. I don't want the impression to be left that the Attorney General has the only determination when we get emergency authority. I am not talking about this particular case we discussed in closed session. But it must be understood that where we had emergency authority, the law requires that probable cause be shown, probable cause that the person we want to target is an agent of a foreign power.

You don't have to go any further than the discussion of the 9/11 Commission recommendations about the difficulties in showing that. It took us so long to get the authority to get the search warrant, to get authorization to search the laptop. It is not an easy showing, and we have to make that showing.

I can tell you once we make it, it is almost instantaneous; it doesn't matter where the Attorney General is, the call is made and he is responsive. If we don't follow that procedure, we are violating the law, and there are felony penalties.

Chairman REYES. In this particular case, people were kidnapped in Iraq, people were communicating about that case. Would that be foreign and—from a common-sense perspective—would be reasonable for a person to assume that probable cause was there?

Mr. WAINSTEIN. Well, I would have to divorce it from the facts here, because it gets into a very sensitive area we can't discuss.

Chairman REYES. I don't want to leave the misperception that people were standing around because of FISA, unable to make a determination. There is a common-sense aspect to every issue that we deal with, including FISA.

Mr. HOEKSTRA. The common-sense approach to that is saying that in FISA probable cause does not extend to an agent of a foreign power in a foreign country.

Chairman REYES. That is exactly right.

Mr. HOEKSTRA. But in this case, the way the communications were reported, they got fourth amendment protections.

Chairman REYES. That is where I disagree with you because, again, American troops were kidnapped in Iraq, communication was taking place in Iraq. The last time I checked, Iraq is foreign. You could assume that it is foreign-to-foreign in that case. I would find it astonishing if any judge said it wasn't ripe for emergency authorization.

Director MCCONNELL. The FISA court said we would not be in compliance. That was the issue. I briefed 260 Members of Congress, and I just failed to make the point.

The point is, someone in Iraq communicating because it passed on a wire through this Nation, this country physically, the law said we had to have a warrant. That is the point.

So what we are arguing is, we shouldn't have a warrant for a foreign-to-foreign country, regardless of where we intercept it.

Chairman REYES. I don't think we have a disagreement on that.

Director MCCONNELL. We can't violate the law. We have to abide by the law. That was the whole point of the reason I brought it up.

We are doing a consideration of probable cause for somebody in a foreign country because of where we intercepted.

Chairman REYES. Which was written into 3356, at your request, and which I will tell you we definitely need to make that——

Director MCCONNELL. Everybody I have talked to is in agreement with the first principle I keep putting on the table. The issue we discussed is when you add the other things. In some cases, it puts us back in the same situation. That was the problem. We didn't have a chance to sit down across the table and say, what is your intent here and what is the probable outcome and how do we pick a better word or different word. We got caught in a time crunch.

Chairman REYES. We are not in a time crunch now. We are going to be able to work with you and hope we cooperate for the good of our national security.

Mr. Holt, you are recognized for 5 minutes.

Mr. HOLT. Thank you, Mr. Chairman. Thank you for holding these public hearings.

Thank you both, gentlemen, for coming today.

I understand, Mr. Director, that you believe strongly that the legislation needed to be changed so that there would be no individualized judicial warrants required for overseas targets. Let me go through a few other things, though.

Did you need and do you need the ability to conduct warrantless searches of Americans inside the United States?

Director MCCONNELL. No.

Mr. HOLT. Do you need or did you need the ability to conduct warrantless searches of domestic mail?

Director MCCONNELL. No.

Mr. HOLT. Do you need to be able to conduct searches without judicial warrants of U.S. persons about foreign intelligence?

Director MCCONNELL. Ask the question again.

Mr. HOLT. Do you need to be able to conduct searches without judicial warrants on persons whose communications might be about foreign intelligence?

Director MCCONNELL. Depends on where and who the person is. If it's a U.S. person.

Mr. HOLT. A U.S. person.

Director MCCONNELL. In this country, it requires a warrant.

Mr. HOLT. And not in this country?

Director MCCONNELL. The U.S. person is protected under U.S. laws.

There is a situation which is covered under Executive Order 12333. You have to have an authorization, but in the current interpretation, that is not a warrant.

Mr. HOLT. Do you need to be able to conduct warrantless searches of library records, medical records, business records, under FISA?

Director MCCONNELL. Not to my knowledge.

Mr. HOLT. Do you need to be able to conduct bulk collection of all communications originating overseas?

Director MCCONNELL. Bulk collection of all communications originating overseas. That would certainly be desirable if it was physically possible to do, since I am in the foreign intelligence business.

Mr. HOLT. Do you need to be able to collect—or conduct bulk communications of someone overseas to an American?

Director MCCONNELL. No.

Mr. HOLT. Do you need to be able to conduct bulk collection of call detail records, metadata for domestic-to-domestic phone calls by Americans?

Director MCCONNELL. Metadata, we think of it as not content but a process for how you would find something you might be looking for. Think of it as a roadmap.

Mr. HOLT. With the exception of that one matter.

Director MCCONNELL. Let me answer your question.

Should I do that without a court order? No. If I do it, I should have a court order.

Mr. HOLT. So would you object to statute language that explicitly prohibits the government from engaging in these things?

Director MCCONNELL. The way we have discussed it in every case you have described, we are prohibited without a court order.

Mr. HOLT. So you would not object, with a clarification of that in the statute?

Director MCCONNELL. Let me go back to my dialogue with the chairman.

As long as we examine the language with a team of experts to understand the consequences and the unintended consequences, I wouldn't object. But what I couldn't do is agree to it without being allowed to read the text or have an expert team examine it, which is the situation.

Mr. HOLT. Now, before the recess and during negotiation over FISA modifications, you issued a statement saying that you strongly opposed the bill that was before Congress, and insinuated it would limit your ability to warn Americans of impending attacks. But later you said you hadn't read it.

Last week, before the Senate Homeland Security and Government Affairs Committee, you said that under the new law you would lose, "50 percent" without the new law, you would lose 50 percent of our ability to track and understand and know about these terrorists.

This week, before the House Judiciary Committee, you said, If we let the new law expire, we would, "lose about two-thirds of our capability, and we would be losing steadily over time."

A week or so ago you said that the new FISA law facilitated the recent disruption of the German terrorist plot, despite the fact this began many months before. You did—after the chairman and I and others made public statements, you issued a public statement.

Let me ask if you understand why some people have raised questions about the credibility of your arguments. Do you understand

that there are some doubts about your ability to act as an unbiased source of information concerning this proposal?

Director MCCONNELL. Many of the quotes you have taken have context to them. There were answers to questions that were specifically framed.

The question I received in the Senate hearing that you make reference to, the question that I understood was, Would the FISA process make any difference; and my answer was, Yes, it did.

That was a key source of information. Once it became politically surfaced, as well as the new law and the old law, the best thing for me to do was just to say, I retract the statement, I will clarify it in another hearing or in closed session.

Did FISA make a difference and save American lives in Germany? Yes. It saved American lives.

Did it matter if it was passed on the 5th of August or earlier? That wasn't my point. It was the FISA process.

My point is, it is more than 50 percent of what we know about terrorists that are plotting to kill people in this country. And the way you frame your question was out of context for what I was trying to respond to in the hearing; and I was trying to be honest and straightforward about it.

Mr. HOLT. Later I will read the full transcript to you, but my time has expired.

Chairman REYES. Thank you, Mr. Holt.

Mr. Issa.

Mr. ISSA. Thank you, Mr. Chairman. I have an article here. I took the liberty of taking a quick glance it. I will ask that it be included in the record at this point.

Chairman REYES. Without objection.

[Article not found]

Mr. ISSA. Thank you, Mr. Chairman.

It is straightforward. It says you can do this. Unfortunately, as I read it—and I would like your read on it, and obviously the Attorney General's office too—what we did when we structured this legislation is, we made it simple, said you could do it; but in the same 105 what we went on to do was endlessly tell you what you had to do after that, within that 72 hours.

If I understand correctly, notwithstanding the chairman's statement that you wouldn't wait 12 hours, you wouldn't take 12 hours if it was your child—and you probably wouldn't; you would be willing to go to jail, you would be willing to violate the law, you would be willing to ignore that to save your own child's life.

That is not the standard we hold people to in law enforcement. We hold them to the standard that they are not—we take them off the cases if it is their child.

As I read the statute, it is pretty clear that you have to have ready a good-faith belief that you are going to be able, after 72 hours, to present to the judge this another 2½ pages of "what ifs" and "notwithstanding" and so on.

Is that correct, Admiral?

Director MCCONNELL. Yes, sir. That is correct. That is the point.

Mr. ISSA. So, in a nutshell, we have talked past each other for the last 45 minutes.

It's pretty clear that if Congress wanted you to have what General Petraeus has—which is, they take our troops, he sends a gunship out, he kills the bad guys, and gets our people back—if they wanted you to have that, they would give you 72 hours to take gunships out, so to speak, without saying, And, oh, by the way, here is what has to be in your after-action for this to have been lawful.

Is that right?

Director MCCONNELL. Yes, sir.

Mr. ISSA. I remember this. And I think General Petraeus has been very good. Everybody who has been over there—as the ranking member has, I have, the chairman—General Petraeus explains that to us; that he can shoot somebody while they are calling the United States, he just can't listen to them while they're calling the United States.

I only put this into record, the Marine online statement, because I think it is important. Notwithstanding the chairman's "We are not going to spy on our troops," I checked and confirmed, and you have in front of you—which I also ask be put in the record anecdotally—that every U.S. Department of Defense site both here and in theater has a warning that says you may be monitored. As a matter of fact, it specifically makes it clear that you will be potentially monitored.

For Mr. Wainstein, I guess my question is, your understanding of how the Uniform Code of Military Justice works when somebody is given a warning like this. When somebody is in theater, is it fair to say their fourth amendment is not, in fact—that, in fact, if they do something inappropriate, including going to a porno site, that that evidence can be used, and they have no expectation of privacy. Is that right?

Mr. WAINSTEIN. Sir, I don't actually have the sheet you passed to the Admiral.

Fourth amendment protections do follow Americans when they go overseas, but obviously if you consent to—you see a banner that says, "By using this, you consent to us looking at it and possibly using it against you if you do anything wrong," if that is what the banner says, then, yes, they have waived that.

Mr. ISSA. I only say that because we are not spying on our troops, our troops are in fact consenting, that for their safety that that happen.

Mr. WAINSTEIN. If we do surveil a soldier overseas who is an American, we have to establish to the Attorney General that that person is an agent of a foreign power.

Mr. ISSA. Of course, if they become a target.

I might, for the record, remind us all that it was insiders—not U.S. troops, but insiders who blew up our mess hall in Iraq; and in fact, they had access or at least the presence of computers and so on.

I think today what we are hearing is, we are hearing the majority say on a bill that they wrote, we didn't cosponsor—they voted for and they sent to the President and the President signed—they are saying, Please don't let us hurt ourselves again, and the American people.

I would hope they don't really mean it.

My understanding of the Rocket Docket in Virginia, it is about 18 months. I just want to have that in the record because I think 12 hours, when you know you are going to a court, the question of speed is highly questionable.

Director, I do have one question for you that is pertinent for both sides of the aisle up here, and that is, all of us who not only receive classified briefings, as we do, but who constantly look to the unclassified Internet information related to areas of study, could not miss that the New York Times and everybody else on and off the Internet has been reporting—with some inconsistency, but reporting—Israel's attack on Syrian sites, and yet members of this committee, having inquired, have essentially been told we won't be briefed.

As much as I want to support you, and I have supported your need to get what you need, I would hope today in an open hearing that you would realize that many of us are frustrated that we do get selective information, and that when you declassified something in El Paso, I respect the fact you did so for what you thought were the right reasons.

But I would hope that we could change the policy, starting today, about selectively handing us little bits of information to tie us up while, in fact, critical information that is already leaking around in an inconsistent way can be brought to the committee that has to make decisions on whether or not our plans and preparations and our eyes on the ground are appropriate.

So if you can comment on that specifically, maintaining an unclassified posture—and I am not talking about the specific incident, but I am talking about the question of how you select answering our questions, including the chairman and ranking member's requests, that seem to be forever waiting to find out and neglected as to whether or not this committee receives it.

Director MCCONNELL. First of all, a very important question. Let me just give you my personal view of the oversight process. Sunshine is a good thing, not a bad thing. So oversight and sharing of information is appropriate and healthy. That is my personal belief in how to engage.

In this specific instance you are making reference to, I would be happy to talk to you about that. There is information at a classified level that wouldn't be appropriate for me to discuss now. There are varying levels of what you can do and not do by agreement between the executive branch and the Congress, so I have to be respectful of that process.

But given the opportunity to engage in dialogue and share information, I am going to default to the sunshine position of making it available.

Mr. ISSA. Okay.

Mr. Chairman, I appreciate your indulgence on the time.

Chairman REYES. Mr. Tierney, I think we have enough time to have you go.

Mr. TIERNEY. Mr. Director, I don't think there has been any disagreement from the beginning as to whether or not a warrant is needed for foreign communications between a person in a foreign country and another person in a foreign country not a U.S. citizen. There is no warrant required.

Many of us have argued consistently that FISA never required a warrant in those situations.

I know there has been some disagreement on that in the interpretation.

I am just going to read the section of the bill that had been filed by the Democrats last session that deals with your issue of whether or not it will clarify that matter. I don't want you to respond now, but I would like for you to submit to us after the hearing your complete reason why you thought the following language wasn't fair enough to satisfy your needs to make it certain that no foreign-to-foreign communications required a warrant.

Section 105(a) reads: "Notwithstanding any other provisions of this act, a court order is not required for the acquisition of the contents of any communication between persons that are not located within the United States for the purpose of collecting foreign intelligence information, without respect to whether the communication passes through the United States or the surveillance device is located within the United States."

So if you would be kind enough to submit to us why you think that is not clear with respect to that issue, I would appreciate it.

Secondly, I think, Mr. Director, you would agree with me—and I think you stated very clearly—Americans and others inside the United States do enjoy constitutional protection or a right against unreasonable search and seizure or interception of their conversations; is that right?

Director MCCONNELL. Right.

Mr. TIERNEY. And it would be unlawful to intercept that communication without a warrant; is that correct?

Then I assume you agree with me that the original program that the President was operating was, in fact, unlawful.

Director MCCONNELL. That is a debate between the interpretation of Article II and Article I. Some would argue it is lawful, some would say "no." I can't resolve a constitutional debate. I am talking about the framework of FISA.

Mr. TIERNEY. Moving forward, we agree, if the government targets an overseas person, a certain percentage of foreign intelligence targets overseas will communicate only with other foreigners overseas.

Director MCCONNELL. I think that is fair to say.

Mr. TIERNEY. Some of them are going to communicate with individuals in the United States, and some of those communications are going to pass through the United States; and it may not, at first, be easy to determine if they are being routed to U.S. persons or to foreigners overseas.

I think that is the crux of the government's dilemma here; is that right?

Director MCCONNELL. That is part of it.

Mr. TIERNEY. Now, the government's been arguing for the agility and speed and says it should not need to prepare applications with particularized orders, meaning specific persons or the specific thing being accepted, for foreign targets overseas. That is the issue that I think these laws have been trying to deal with.

Still, you will agree with me, I think, that when the government listens to both ends of the communication, one in the United

States, as it admits it has done, and probably will do, even if inadvertent, in the future, it does infringe on the privacy rights of American citizens.

The question is whether or not that infringement is reasonable.

Director MCCONNELL. Sir, the issue for us is, you can only target one end of that conversation. You can't control who that person might talk to.

Mr. TIERNEY. Exactly. So, for this purpose, the government has put in some selection and filtering methods.

Director MCCONNELL. The issue is who you target.

Mr. TIERNEY. Well, the issue is not who you target; you are going to target foreigners overseas, but sometimes they are going to have communications that go through the United States. So the issue is, what are you intercepting.

Director MCCONNELL. That is correct. The old law was, if it touched wire here, we had to have a warrant against the foreign target. That was the issue.

Mr. TIERNEY. Mr. Baker, who, I think you will agree with me, is an expert on the legislation and implementation of FISA—at least your general counsel, Ben Powell, said he was an expert in front of the Judiciary Committee——

Director MCCONNELL. He is an expert.

Mr. TIERNEY [continuing]. He indicates to us in his testimony that it wasn't a situation of technology that really is the issue here. He says that, contrary to the history earlier, Congress anticipated fiberoptics and cable usage in overseas conversation when it did FISA back in 1978; but the real issue is, who is the decision-maker for authorizing what it should be, what level of justification should be required, and what standard of review should the decision-maker apply, how individualized authorizations to conduct surveillance should be, and what role judges should play in this process.

He testified that in many situations over the years aggressive and well-meaning attorneys throughout the government pushed aggressive interpretations of the law to make sure we balance its reasonableness.

The government has these selection and filtering methods. The question is whether the government's criteria for determining selectors and filters result in methods that are likely to assure that communications being intercepted are to and from non-U.S. persons overseas and whether those communications contain foreign intelligence.

Now, even that is backing off of the requirement that it—if you are a foreign agent or an agent of a foreign power, it broadens it out. But assuming we are going that far on that, it is probably more important that we have adequate protection.

Is there any reason why that determination of reasonableness, whether or not those filtering methods are reasonable, shouldn't be left to a court as opposed to you, sir, as the DNI, and the Attorney General?

Director MCCONNELL. They are under the law as signed in August; they are subjected accordingly.

Mr. TIERNEY. After the fact, significantly after the fact. And then the standard is "clearly erroneous." It means you have to give in-

credible deference to the administration, not just the usual deference.

Is there any reason in your mind why that could not be subjected to judicial review at a reasonable standard?

Director MCCONNELL. The issue I would object to is submitting it to the court before we can engage in conducting our mission.

Mr. TIERNEY. You are already engaging in your mission right now. So if we were going to have a law at a future date, is there any reason under that system the judge could not first determine whether or not those selection and filtering processes were reasonable?

Director MCCONNELL. I would object to having courts be between us, conducting the mission and giving us permission in the way you describe it, foreign person, foreign country.

Where it is now, the court will review it, as you mentioned, after the fact of procedures, to make sure we are doing it right.

Mr. TIERNEY. Let's have the procedures approved before they go into effect.

Director MCCONNELL. Then you get us in a situation where we were discussing earlier, with getting the emergency procedure.

Mr. TIERNEY. But you already have a law in effect right now.

Director MCCONNELL. We have the law in effect, which changed the hypothetical you are setting up.

Mr. TIERNEY. I am talking about going forward. You have a law in effect and you are collecting now.

Director MCCONNELL. That is right.

Mr. TIERNEY. So going forward, is there any reason why a court couldn't review for future use whether or not your methods are in fact reasonable?

Director MCCONNELL. What we are targeting changes all the time. So if you put the court between us and the foreign targets, then that——

Mr. TIERNEY. We are putting the court in a determination of whether or not your selection and filtering methods are reasonable.

Director MCCONNELL. Which is in the law now.

Mr. TIERNEY. Whether or not your determination was clearly erroneous, which is an entirely new standard from matters of fourth amendments rights.

Mr. WAINSTEIN. Sir, may I make a quick point on that?

Mr. TIERNEY. Only if I could get the Director's answer on that first.

Director MCCONNELL. Sir, what we tried to accomplish was having the court look at the procedures in a reasonable way.

Mr. TIERNEY. Why did you accomplish not allowing the court to make a determination as to the reasonableness of those selections and filters?

Director MCCONNELL. I am not objecting to that so long as it's not in advance. Our world is very dynamic.

Mr. TIERNEY. You have no objection to the court making the review as to whether or not your selection and filtering methods are reasonable.

Director MCCONNELL. Reasonable.

Mr. WAINSTEIN. If I could, just very briefly, the law that you passed requires that; but the standard, as you pointed out, is clear-

ly erroneous, and you said that is a new standard. That standard is actually in FISA, the original FISA.

Mr. TIERNEY. But not in this application, not with respect to whether or not you are looking at the selection and filtering methods. It is a significant departure downward from a fourth amendment requirement that warrants it be based on reasonableness.

Mr. WAINSTEIN. Sure. It is a different animal.

Mr. TIERNEY. Not that much of a different animal. We are talking about interception of communications of people in this country, of U.S. citizens. So the reasonable standard there is no reason—as I understand the Director now saying, he has no objection either—that the court look at that for the purposes of reasonableness.

Mr. Director, do you have any objection to the court actually looking afterwards at the reasonableness of the mitigation aspects that are put in play?

Director MCCONNELL. A review after the fact, no.

Mr. TIERNEY. Do you have any objection to the inspector general auditing the performance of the government under this law, or whatever law might come along, so it can report to Congress on what has transpired under the act?

Director MCCONNELL. I would have to understand exactly what that means. There are about four levels of review now.

Chairman REYES. If I could interrupt, we have got three votes. We are going to have to recess. You are certainly welcome to come back.

Mr. TIERNEY. One question and I will be done.

Do you have any objection to the inspector general's office doing a review or reporting to Congress on the implementation of this law?

Director MCCONNELL. If it was something requested by the Congress as part of the Congress' duties, that is something you could request. I think the standard we have now established is sufficient because there are four levels of review.

Mr. TIERNEY. The standard right now is that the executive will watch over the executive and report about what the executive is doing.

Director MCCONNELL. No, sir. It involves the court and it involves the Congress.

Mr. TIERNEY. We can have a discussion, if the chairman wants to leave; but I can tell you, it has not in any semblance of satisfactory manner, in my view.

Chairman REYES. We have three votes. We are going to recess. We should be back in about 20, 25 minutes.

The committee stands in recess.

[Recess.]

The CHAIRMAN. The committee will please come to order.

And the next speaker will be Mr. Ruppersberger, who will be recognized for 5 minutes.

Mr. RUPPERSBERGER. Mr. Director, first I think that this is an issue that we should come together, Republicans, Democrats, as a country, and that is why we are having these hearings. We know we are rushed through, but we do need to resolve some of these issues.

There is no question that everyone here is going to get the tools pursuant to our Constitution to be able to fight terrorism. But, you know, I think the big issue, the big dispute is the issue of oversight.

Our forefathers created a great system of government with checks and balances. And we need to continue those checks and balances as it relates to Americans.

That is what our men and women in the military fight for, for our freedom and liberty and also our Constitution.

Now Director McConnell, I would like to ask you three issues: You said that you needed three components to deal with what we have. Number one, no individual warrant for foreign targets; would you agree?

Director MCCONNELL. Yes.

Mr. RUPPERSBERGER. A way to compel the private sector to assist surveillance.

Director MCCONNELL. With liability protection.

Mr. RUPPERSBERGER. And three, a requirement for individual warrants when targeting Americans.

Director MCCONNELL. A U.S. person, yes, sir.

Mr. RUPPERSBERGER. Yes. Not foreign.

I think it is very clear in the old law and what we are talking about now that we don't need a warrant as it relates to foreigners.

Director MCCONNELL. A U.S. person can be a foreigner if he is in this country. A U.S. person and foreigner, even a terrorist suspect, would get that protection if he is in the United States.

Mr. RUPPERSBERGER. That is up to interpretation. We need to clarify these laws, and that is why we are here to write the laws. And right now, I think just the President's statement yesterday, there is no clarity.

I happen to represent the district where NSA is located, and I am the chairman of the committee that oversees the NSA. So a lot of the people that work at NSA are my constituents. They need clarity. They need to go to work and know what is right and wrong and know what these issues are——

Director MCCONNELL. I fully agree.

Mr. RUPPERSBERGER. Now with these three components, it is my belief that the negotiations that we had in the Democratic bill, H.R. 3356, addressed all of these issues. Do you feel they did or did not?

Director MCCONNELL. No, sir, not when you extend some of the language to the impact, and that was our issue.

Mr. RUPPERSBERGER. I believe from what I have heard today that we are very close to resolving the issues.

The one point is the oversight. And I can say this: This issue that has been used about Iraq and Americans kidnapped, that is a leadership, that is a command issue. We—this law will allow us to react at any time. And all we are doing, and I think people misunderstand the fact that there is so much volume that has to be done in these very rare circumstances, and the testimony that we have clearly has persuaded me that we in no way need to have even probable cause if there is an emergency situation that exists and you can act upon that and you need—you can act upon that.

However, you have the 72 hours to develop, so the court oversees it. But the court is only overseeing process, not each individual case. Would you agree with that?

Director MCCONNELL. In the old law, we had to have probable cause that would stand up. In the new law, which was signed in August, we would not have to have now a warrant for a foreign person, foreign country. So that situation wouldn't arise again under the current law.

Mr. RUPPERSBERGER. And yet we have no judicial oversight. That is the issue. That is not the system our forefathers created.

You have said that you agreed that the courts should be involved in reviewing procedures for surveillance that may involve Americans after the surveillance begins, correct?

Director MCCONNELL. I am sorry. I couldn't quite hear you.

Mr. RUPPERSBERGER. You have said that the court should be involved in reviewing procedures for surveillance that may involve Americans after the surveillance has begun.

Director MCCONNELL. No, sir. Not exactly. The law says, currently, if it involves U.S. persons, we get a warrant. So that is a decision up front that now—I think what you are describing, the law now subjects to the court review of our process and procedures to make sure it is consistent with the law. I agree with that.

Mr. RUPPERSBERGER. You agree with that.

Let me get to one other thing. Wire taps.

I used to do wire taps as an investigative prosecutor, always with the courts, dealt with the telecom companies.

You can't have wire taps if you don't have their support and they need to work with you. And I agree that there should be some type of immunity as it relates to the telecom companies because they are really acting on behalf of the Nation as really an agent of the United States.

But here is a problem that we have. To just say you want immunity is not enough. We want to know what we are giving immunity for. And unless we get the documents that we have asked for, I can't understand why there is a resistance to give us the information that we want to see from the administration, and if we get that, I believe that we might be able to come together and to put together a bill very quickly on behalf of our country and give our—the resources that we need to deal with the issue of terrorism.

Now please address the issue of why we have not been able to receive this information. We cannot give blanket immunity until we find out what we are giving immunity for. Could you please answer that?

Director MCCONNELL. Sir, all I can say is it is not something I am responsible for. I made my recommendation. It is a subject under current dialogue between the various committees.

Mr. RUPPERSBERGER. Would you make recommendations to the administration to give us information so that we can make a decision on the immunity?

Director MCCONNELL. My recommendation is to give the Congress access to what they need for the oversight purposes.

Mr. RUPPERSBERGER. Would you be continue to be very strong in your recommendation to the President?

Director MCCONNELL. I am strong in that because I believe it.

Mr. RUPPERSBERGER. If we can see that, then we might be able to resolve this entire issue without the anxiety and the President going to NSA and talking about lives at risk. We all care about American lives, and we will do what we have to do to protect them.

Thank you.

The CHAIRMAN. Thank you.

Ms. Schakowsky.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

Director McConnell, I am wondering, first, if you would provide to the committee in classified form specific instances of how NSA or the Intelligence Community was prevented altogether from collecting foreign intelligence prior to the passage of the PAA?

You say those words, prevented altogether, on page 6. Mr. Wainstein says prevented altogether on page 5 of his testimony.

So I would like to know how the law prevented altogether in which instances you were prevented from the ability to collect foreign intelligence.

And I would also like to know when you present that to the committee in classified form, how H.R. 3356 did or did not correct that problem.

So that is a request. Would you comply with that request?

Director MCCONNELL. Yes, ma'am.

Mr. WAINSTEIN. I could answer that right now if you would like.

Would you like an answer to that?

Ms. SCHAKOWSKY. I would imagine that there are specific instances that you would want in classified session, but if you want to briefly answer that.

Mr. WAINSTEIN. I think it is important to note that one of the things that is required when we have to go through the FISA court is we have to show probable cause that the person we want to target is an agent of the foreign power, and the rest of our signals intelligence collection, we don't have to do that. That is a big burden.

Ms. SCHAKOWSKY. But I would like to know, and that is why I would prefer to have it in the classified form because I want to know the times that you were prevented from doing that.

Mr. WAINSTEIN. I understand. But just in the abstract, there are a number of instances where we cannot make that showing and we could not therefore do that surveillance, and that is one of the issues that we had with the bill.

Ms. SCHAKOWSKY. I want to assure myself by seeing those instances.

Director McConnell, we have been repeatedly told that the rights of U.S. persons would be protected under the new authorities because the NSA would minimize—you talked about minimization—U.S. person information.

So will you commit that you will be able to tell us how frequently U.S. person information gets collected under the new act?

Director MCCONNELL. We will look at the information and see what can be made available. As I tried to explain in a similar question earlier, we may not be able to even answer the question, but what we can find we will provide to the committee.

Ms. SCHAKOWSKY. Okay, then, and will you be able to—will you commit to that? You will be able to tell us how many times U.S. person information gets disseminated under the new act?

Director MCCONNELL. Yes, ma'am. That is an easier thing to do.

Ms. SCHAKOWSKY. Will you be able to commit that you will be able to tell us how many times information gathered under the new act gets used to seek FISA warrants under U.S. persons?

Director MCCONNELL. That would be a relatively straightforward thing, yes.

Ms. SCHAKOWSKY. So you may not be able to tell us how much U.S. person information gets collected under the new act.

If you are unable to answer that basic question, how is this committee going to be able to do proper oversight to exercise our constitutional mandate to do that kind of oversight to protect the rights of Americans?

Director MCCONNELL. Ma'am, as I tried to explain earlier, it may be incidental collection. You don't—there is no human that is aware of it. So you wouldn't know that until you went into the database. That is why I was saying to answer your question specifically, it may not be an answer we can get. Now once there is some reason to look at data, then we can—we keep track of that—we would certainly be happy to provide it to you.

Ms. SCHAKOWSKY. Okay. So there may be information about Americans in that database.

I am looking at your testimony before the Judiciary Committee on Monday, "I am not even sure we keep information in that form. It will probably take us some time to get the answer."

And then later you say, "it might create a situation where it creates significantly extra effort on our part."

I think the protection of the privacy rights of U.S. persons is worth effort. I mean, if names are in a database and they are sitting in a database of innocent Americans, it would seem to me that that would be something this committee, that this Congress should be able to have oversight on.

Director MCCONNELL. Ma'am, let me try to put it in a context, maybe use an example, make it a little easier to understand. There are literally billions of transactions.

Ms. SCHAKOWSKY. But how do you know it is incidental if you don't have the statistics?

Director MCCONNELL. In the context of foreign intelligence, we can't control what foreigners might say about Americans. Frequently, there is a reference to political figures in the United States or something. We may not know that is in the database until we have some reason to go query that portion of the database for foreign intelligence purpose. So it could be there and us not be aware of it. That is the point I am trying to highlight.

Where it has been used or specifically excluded from the database, we probably can provide those numbers. I just don't know the extent of it, but I will be happy to look at it and see what we can provide to you.

Ms. SCHAKOWSKY. You know, Mr. Chairman, let me just say that on a number of occasions, we have found that databases have collected private information about American citizens, and later on, then, well, we made a mistake; it shouldn't be there; we should get it out of the database.

I would prefer to see that at the beginning of the process that we make sure that we protect people's rights and that that become a priority regardless of the effort that it may take.

Thank you, Mr. Chairman.

The CHAIRMAN. I thank the gentlelady. We will pursue that from a committee standpoint.

Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman, and gentlemen, thank you for your testimony here today.

I appreciate the difficult job that you have on your hands and all that you are trying to do to protect the American people.

We are in this together, and we want to make sure, of course, that you have the tools that you need in order to protect the country. It is equally important we want to make sure that we are protecting the rights, the civil liberties of the American people. And that is what the struggle really is all about. What is the right balance. And I think we are all on the same page; we are very close on most of these issues. We clearly—there is a unanimous agreement here that we don't need a warrant for foreign-to-foreign communications, and I want to make that clear for those that are watching.

I did want to get into some of the questions with respect to surveillance of insurgents and the example in Iraq that had been given.

Correct me if I am wrong, but "insurgent," by its very definition is to qualify as an agent of a foreign power. So when you are talking about, you know, justification for probable cause, that is your probable cause, right?

Director MCCONNELL. Yes, sir. It is the process of going through that and submitting it to the court is the issue.

Mr. LANGEVIN. So it is not a heavy lift to prove that that is a——

DIRECTOR MCCONNELL. My point is it took time and then it had to satisfy a court for probable cause standard. That is what I was trying to highlight.

Mr. LANGEVIN. I want to get into the process part of this. One thing where we haven't drilled down into is the fact that the process really there is really two parts of it. There is the legal or management or judicial part of the process, and there is the technical part of the process. And clearly, either before the Protect America Act was passed or after, although it clarifies and as did the House bill that we passed, that there was pretty much we believe that that satisfied all of the three requirements that you said that you needed; and we bent over backwards to try to make sure that we gave you what you needed in terms of being able to conduct proper surveillance and at the same time protecting civil liberties. That House passed bill solved the management and the judicial part of it, but the reality is even the Protect America Act did nothing to change the technical aspects or the steps that need to happen physically in order to do surveillance.

Director MCCONNELL. It took away the requirements for probable cause.

Mr. LANGEVIN. That is a management change. That is the judicial change. But we talk about the delay that, even in surveillance, it is—there are still technical things that happen that take time.

Director MCCONNELL. No question. It is automatic.

Mr. LANGEVIN. So I wanted to—the Protect America Act, even that went only so far. I mean, there are still——

Director MCCONNELL. Still going to take some time, no question.

Mr. LANGEVIN. I wanted to clarify that for the American people for those who are watching.

While I still have my time, Director McConnell, on September 17th, this committee had received a letter from—actually, let me go into another area because I was going to—I don't have that much time left.

You had made various statements, sometimes, that seem to be inconsistent in the whole process when we were deciding between the administration bill and comparing that with the—with 3356, the Reyes-Conyers bill.

For example, on August 3rd, 2007, the eve of the House vote on H.R. 3356, you issued a statement claiming that the House proposal was unacceptable and that the bill would not allow you to carry out your responsibilities to provide wanting to protect the Nation.

Yet during a recent interview with the El Paso Times, you noted that you never had a chance to read the bill because again it was so complex.

Can you clarify which of those statements are accurate? I am looking at your—the statement that you had on the Web site, and I can read it, if you need me to.

But can you clarify it for——

Director MCCONNELL. Sure. I would be happy to.

In the final flurry, there were seven bills exchanged I think: four from the administration and three from the Congress. So what I might have been referring to was the situation in the Senate when what we were facing in the last few moments was very senior people calling me saying, do you agree to these points.

What I was trying to go back to are the three philosophical points or fundamental issues you had highlighted earlier which is my point of view. I had a team of 20 or so lawyers that are technical experts in aspects of it. So once we had examined the House bill, there were portions of it that inserted ambiguity and you—you slipped into it a moment ago. You said foreign-to-foreign. Many would like to say it is okay if it is foreign-to-foreign. What I keep trying to highlight for the committee is you—is you can only target one thing. You have no control over who the person at the other end of the phone is going to call or who is going to call that person.

So the language that was in 3356 inserted ambiguity and uncertainty. We weren't sure it would come out the way we needed it to come out to do what we thought to protect the nation.

Mr. LANGEVIN. Did you in fact read the House passed bill?

Director MCCONNELL. I personally skimmed it over. Did not read it in intimate detail. I said I had a team of 20 lawyers that know every piece of it, were examining the intended and unintended consequences.

So any statement that I issued would have been a result of that process.

Mr. LANGEVIN. I just want to point out that both the House passed bill and the administration bill were each six pages long, so it is not a heavy lift to read through it thoroughly.

Director MCCONNELL. I understand that, sir, but let me highlight the definition of electronic surveillance. What we were attempting to do is to get foreign—"target foreign country" excluded from that definition. If you don't exclude it, then it has consequences throughout.

Mr. LANGEVIN. My time has expired, but I wanted to clarify that clearly my opinion both then and now, that is exactly what the House bill did, gave you the things that you needed to do to exclude foreign-to-foreign, and it was not an issue.

Director MCCONNELL. I will be happy to go sit down and go through it and let you see our point of view and your point of view and see if we can agree on some language.

Mr. LANGEVIN. I hope we can do that.

I yield back.

The CHAIRMAN. Ms. Wilson.

Mrs. WILSON. There has been some discussion here about using common sense and that, particularly in cases of emergency, people should use common sense and that we should listen to people overseas particularly in a case where someone has kidnapped our soldiers.

Mr. Wainstein, is there a common sense exception to the requirements under FISA?

Mr. WAINSTEIN. No, ma'am. The requirements are pretty stark and clear, and there are criminal penalties if you violate them.

Mrs. WILSON. So if someone said, look, this is a—this is an emergency with all reasonable people here, we know we have got to find these guys, let us go up on the number and we will take care of the paperwork later. Would that be a felony?

Mr. WAINSTEIN. It would be.

Mrs. WILSON. Are you willing to commit a felony?

Mr. WAINSTEIN. No. As a public servant, I cannot violate the law. Though I understand the thought that it would be nice under those circumstances to do whatever is necessary to save American lives, the reality is that we can't do that.

Mrs. WILSON. In the case where you have got an analyst forward who perhaps is located in Baghdad who had—thinks that he had something. Thinks that he had something that might be able to help in an emergency situation, knows it is an emergency situation, can he pick up the phone and call you and say, hey, I have got something here, it is really important, this is why I think that?

Can you sign off on it if that in reality happened?

Mr. WAINSTEIN. It does happen. These calls go straight into the folks who work directly with me. They get right to me and get right to the Attorney General. That actually happens in a very short time. What happens is they have to have the information necessary to satisfy the probable cause standard.

Mrs. WILSON. So they have to be able to show you that they have probable cause to believe that this guy in a foreign country is affiliated with a foreign power and so on and so forth, all of the requirements that are set out in the statute?

Mr. WAINSTEIN. Exactly. And if I played this out, if we go ahead and authorize emergency—grant emergency authorization to go ahead and go up on surveillance, and within 72 hours we are not able to satisfy the probable cause standard to the FISA court, that surveillance goes down. We lose that surveillance.

There also are penalties in that statute to say that—there is a presumption that we have to notify the target that we have been surveilling him.

Mrs. WILSON. Let me make sure I understand this.

So if we move too fast, we didn't meet the probable cause standard for a foreign person in a foreign country, it was probably an insurgent, and the FISA court here in Washington says, "No, you didn't meet that probable cause standard," we would actually have to go out and find the insurgent and tell them that we were trying to listen to them?

Mr. WAINSTEIN. In theory, we would. There is a presumption that we actually notify the target of the fact of the surveillance which, if you can imagine, would really compromise our intelligence operation.

So it is because of that and just because we have to adhere to the law, we take that responsibility very seriously to make sure we have the sufficient evidence, no more than bare sufficiency, but we have sufficient evidence to satisfy probable cause.

Mrs. WILSON. And the Protect America Act fixes these problems?

Mr. WAINSTEIN. Yes, for targeting people overseas it does,

Mrs. WILSON. When was this committee first briefed on the particular case that we have been talking about? Do either of you remember?

Director MCCONNELL. I can get back to you. I just don't remember. It was actually briefed back to you by another group in our community, and I don't remember the exact date.

Mrs. WILSON. Do you remember about when?

Director MCCONNELL. I would say probably—our people back here think it was May, but I will get you the specific date.

Mrs. WILSON. I believe you are correct.

I want to thank both of you gentlemen for your work on behalf of the country.

I would ask one final question. The Attorney General is required to report on all electronic surveillance in the United States conducted under the Foreign Surveillance Intelligence Act as amended every 6 months to this committee.

Will you provide that information and will you continue to provide that information to the committee as required by law, Mr. Wainstein?

Mr. WAINSTEIN. Yes. Absolutely. And we will also do the additional reporting that we have agreed to do in regard to the Protect America Act.

Mrs. WILSON. Could I continue to go out to the National Security Agency, as I have before, and be given open access to all of their cases with respect to satisfying for myself that you are following the law?

Mr. WAINSTEIN. Absolutely.

Director MCCONNELL. Yes, ma'am.

Mr. WAINSTEIN. If I may, Mr. Chairman, briefly correct one thing.

When I told you about the provision that says we have to notify the target if we go up on emergency authorization and don't end up getting court authorization, that request is limited to U.S. persons.

So let us say we have a U.S. person who is an agent of a foreign power and we go up on that person overseas, we would have to notify him. I think because the hypothetical you posited was an insurgent, in the case it is not a U.S. person insurgent, we wouldn't have to.

Mrs. WILSON. But if it was a U.S. person overseas that we were tracking and we went up too quickly.

Mr. WAINSTEIN. Yes. We would have to, and not only does that have practical consequences but it reflects the seriousness with which Congress and the court takes our assessment of the evidence of the front end to make sure there is probable cause.

Mrs. WILSON. Thank you very much, Mr. Chairman.

The CHAIRMAN. Thank you for clarifying that up because I was going to ask you that very same question.

Mr. Holt.

Mr. HOLT. Thank you, Mr. Chairman.

Mr. Director, you said that emergency provisions under FISA still have to meet a probable cause standard.

Director MCCONNELL. Earlier but not now.

Mr. HOLT. So what standard do they have to meet? Is it the hunch of a political appointee? Is it the firm belief of a dedicated professional in the middle of the administrative change? I mean, who has the responsibility?

Director MCCONNELL. For determining——

Mr. HOLT. If it is not a probable cause standard, what standard is it, and who applies that standard?

Director MCCONNELL. For a foreign target in a foreign country, is that the question?

Mr. HOLT. The standard that justifies intercepting and storing and maybe in the future analyzing a communication.

Director MCCONNELL. For a foreign target in a foreign country——

Mr. HOLT. For any of that who is determining whether it is a foreign target to determining whether there is someone whose conversation should be intercepted.

Director MCCONNELL. Since our mission is foreign intelligence, the standard would be enforced by the analyst working the problem against a foreign target in a foreign country.

Mr. HOLT. And if this person who is responsible for it knows that there is no judicial oversight, not in 72 hours, not ever, do you think this person will make the decision differently under this law than the person would have made it under, say, FISA?

Director MCCONNELL. No. I don't think so.

Mr. HOLT. So the FISA law would have been just fine because operationally the person wouldn't make the decision any differently under this law. I believe that is what I just heard you say.

Director MCCONNELL. That is not correct, sir. I would like to respond to that.

The issue we are discussing is, do you have to have probable cause submitted for an approval process for a court on a foreign person in a foreign country. That is what we are trying to highlight here. It is not the way you framed it.

Mr. HOLT. What I was asking was, who makes the decision and who overseas that decision? Who provides protection against the kind of thing that we see in oppressive governments around the world, a knock on the door in the middle of the night, somebody barges in and searching the place? Now we are talking about figuratively, an electronic search, maybe not a physical search, although maybe we are talking about that in this legislation.

The question is, who provides the kind of check and balance that Americans expect that will protect them against having their lives ruined by an overzealous government who is trying to protect the safety and security of the people?

Director MCCONNELL. Three levels of protection——

Mr. HOLT. Or would protect them from a government who would have an enemies list which you might say that it never happens here, but it has.

So the question is, who provides what standard, and you just said, I thought, that operationally the person would make the—the person who does make the decision that it is okay to tap this phone or to intercept that communication would not make a decision any differently if the court were not looking over his shoulder if they were not required to have a warrant either now or maybe 72 hours later.

Director MCCONNELL. Three levels of protection. First of all, the initial judgment would be made the same way it has been made for almost 30 years. That is—that is the professional that is doing the mission. It would be then reviewed internal to that organization. It would be reviewed by the Department of Justice, and as passed in the law last month, the procedures for doing that would be reviewed by the court.

The last level of oversight is this body, this committee. You can walk at any time out to NSA, look at anything you want to——

Mr. HOLT. But you just said you can't give us that information. You said to Ms. Schakowsky, you said you don't even really know whether—who we have intercepted.

Director MCCONNELL. I said it might not be knowable. We can look at it and see if it is a knowable answer.

Mr. HOLT. So that is not much reassurance to us so we have to exert that oversight that no one else along the way is exerting except a well-meaning political appointee, or maybe not so well-meaning political appointee, or well-meaning but perhaps mistaken bureaucrat. These people are trying to do their jobs. They are trying to protect us. But we have to give them the guidance.

Now one of the things that concerns us is that, you know, the Intelligence Community, you are particularly, more than anyone else in the United States, supposed to speak truth to power. And that means you have to keep a certain distance from that power to whom you have to speak the truth. And that is why it concerns me that when you talked about the lawyers who were working to prepare this legislation back in August, when you made the—some of the statements that you made, they clearly seem to be influenced

by lawyers in power in the White House, in the Vice President's Office. And that is troubling, actually.

You, of course, are a Presidential appointee, but it is critically important that you keep a professional distance. That is why I asked these questions earlier today that I am afraid you might have thought were insulting. But your credibility as an independent person is so important to our safety and security, so important to our rights as humans.

So, I mean, can you say that during those hours when this legislation was not—was being written that your team of lawyers was not consulting with, say, Mr. Addington and his team of lawyers?

Director MCCONNELL. I would say it was not influenced by a political process. I spoke truth to power. There is a team of lawyers that worked this starting last year and a team worked it throughout the past year and up to including the period of time that we had the bill passed in August.

Mr. HOLT. How much consultation was there between your lawyers and the Vice President's lawyers?

Director MCCONNELL. With the Vice President's lawyers, there was extensive consultation with the lawyers working the problem. I don't know who was working the problem in the Vice President's Office.

Mr. HOLT. Forgive me if this seems insulting, but you have to take a step back about what it means to be able to speak truth to power and to have an independence in what we say that is permissible to do with Americans' lives.

Director MCCONNELL. I did.

The Chairman. Thank you, Mr. HOLT.

Mr. Tiahrt. First round.

Mr. TIAHRT. Thank you, Mr. Chairman.

This year, in a bipartisan fashion, we passed the Protect America Act. It passed the House. It passed the Senate, signed into law by the President.

Would you—what would the impact on the intelligence collection be if the Protect America Act were not renewed?

Director MCCONNELL. We had lost half to two-thirds of our capabilities, specifically targeting terrorist groups because of the, not the court, but the language of the law that the court had to interpret, and within a few days after passing the act, we were brought back up in full coverage.

Mr. TIAHRT. So the Protect America Act has helped enhance the speed and agility of the Intelligence Community?

Director MCCONNELL. Significantly, yes, sir.

Mr. TIAHRT. Okay. That is good news.

Now we heard privacy advocates outside and inside the committee that have argued that the minimization processes are inadequate to protect Americans' privacy interests. They take issue with the fact that the government may still capture and screen incidental communications as we just heard and even if no use is ultimately made of the contents of those communications.

Do you feel that the procedures adequately limit the government's intrusion into the protected communications of America?

Director MCCONNELL. Sir, I do, because intrusion would be a violation of law. So the minimization procedures have been in effect

for almost 30 years. They work and work well. I had the pleasure and the privilege of serving as the director of NSA, so there is a whole training, oversight recertification program about how you would do that. And so it has worked well. It has been subject to the court and reviewed by the court and endorsed by the court. So it has worked for almost 30 years.

Mr. TIAHRT. Is there a practical alternative to what you are doing now?

Director MCCONNELL. No, sir. There isn't. That is one of the reasons that we failed to communicate on one of these issues. Often someone would say, well, it is okay to do foreign-to-foreign, and what I keep attempting to highlight you can only target one end of the conversation. You can't control who that person at the other end might call. An overwhelming majority, I don't know the number, but it is almost always—it would be a foreign-to-foreign communication but can't guarantee it is.

So if you make it a condition in the law that you have to guarantee it ahead of time, it effectively shuts down your operation. So in the condition that a foreigner called in and there is incidental collection, then it would be minimized. If it is nothing of harm to the Nation, it would be minimized. If it was potential harm to the Nation, that might be our most important call, then we would take appropriate action.

Mr. TIAHRT. If a terrorist is being monitored internationally outside of the United States and somebody from the United States calls into that terrorist's phone number and there is, in the mind of the agent, a probable cause to investigate that contact, what is the—for that citizen inside America that has made the phone call, is that handled by your agency, or do you turn that over to the FBI to develop probable cause and complete the investigation?

Director MCCONNELL. On the way you have described it, the target for my community would be the foreign person, foreign country.

Once that call is made, as it was in the 9/11 situation, it would—subsequently reported on 9/11 and joint commission of Congress—that call was made, then Intelligence Community would realize U.S. person calling a terrorist, depends on the contents of the conversation.

If it turns out it is a terrorist operation planning whatever, refer to the FBI. The FBI would get a warrant against the U.S. person, the person located in the United States and then do their normal surveillance mission.

Mr. TIAHRT. So they would carry out the requirements of the Fourth Amendment of the Constitution as far as probable cause?

Director MCCONNELL. Yes, sir. Under a warrant subjected to court review.

Mr. TIAHRT. The committee received testimony earlier this week that the FISA court should have to make probable cause findings to protect every person who might potentially communicate with the target and not just the target itself.

In other words, an incidental contact, that probable cause would have to be achieved. What is your reaction to that proposal?

Director MCCONNELL. Effectively, sir, it shuts down our operation because it creates a condition we couldn't satisfy in the eyes of the law. So that is why we are arguing for exclusion of where

is the target and the target overseas, and as I mentioned earlier, what we were—what we were caught in, in the old wording and the old law, is because of where you intercepted it in this country, this is what caused the problem. If it had been intercepted in the foreign country in a different mode, wireless, it wouldn't be a question.

Mr. TIAHRT. So a majority of the contacts of communications of the target—let me put it this way. Does foreign target communications mainly deal with foreigners and their contacts?

Director MCCONNELL. Almost always.

Mr. TIAHRT. Almost seldom that it isn't?

Director MCCONNELL. It is a very tiny fraction of the percent.

Mr. TIAHRT. And when it does occur and there is probable cause, it is turned over to the FBI.

Director MCCONNELL. And if it were incidental, meaning they call a pizza shop, that is of no intelligence value, you take it out of the database.

Mr. WAINSTEIN. If I could add to that very briefly.

In the argument that you have heard occasionally, when somebody we are surveilling appropriate under this statute called somebody in the United States, that should then trigger a requirement for the government to get some kind of court process against someone in the United States.

While that sort of has some gut level appeal when you first look at it, you have got to recognize that that is not the requirement in any of the regimes.

For instance, on the criminal side, title three warrants. You get a title three warrant against one person, that has the—that gives you court authority to surveil that person. That person talks to somebody else, another American, we don't have to go back to court to get approval to listen to that person's communications. So that is the way it is on the criminal side and on the foreign intelligence side. And as the director said, that is the only workable way to deal with it. We just deal with it with minimization instead.

Director MCCONNELL. If you make that other person your target now, you are going to listen to him intentionally, that becomes subject to a warrant.

Mr. TIAHRT. For the record, I would like to say that I think it is important that your lawyers communicate with those in the—other parts of the administration, and we should not limit free speech when we are developing policy or looking at how we apply current law. So to limit context in free speech in order to make us move forward in this process, I would be opposed to that limits on free speech. I think you should be in contact with other areas of the government and we shouldn't restrict it.

Thank you for your testimony.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Mr. Tiahrt.

Mr. Tierney.

Mr. TIERNEY. I am glad you made that last caveat. Because if we have significant interception on a U.S. citizen or person in the United States, then, of course, you would need a warrant. And I think we should all understand that.

Director MCCONNELL. If they are the target.

Mr. TIERNEY. It is determining when that cross-over point is.

You also at one point in earlier testimony said that there were perhaps billions of data or records, transactions, being done. So when you talk about a small percentage, it is a small percentage of those billions that might sort of scoop in——

Director MCCONNELL. When I was talking about billions of transactions, we would have some subset of that; and when you work it down, it turns out to be a pretty small number.

Mr. TIERNEY. So a small percentage of the billions in the subset, it still could be a substantial number. That is the problem.

Earlier this week, we got a letter from Mr. Alex Joel. I understand he is your civil liberties protection officer in your office; is that correct?

Director MCCONNELL. That is correct, and I think he is with us.

Mr. TIERNEY. It lays out the civil liberty and privacy protections that he believes his office is charged with overseeing in the implementation of the new Act.

I indicated earlier that one of my problems is I don't think it ought to be the DNI's office overseeing the DNI. But set that aside for a second. Mr. Joel's letter states, among other things, that although he doesn't read the PAA to require it, the NSA is still using the minimization procedures that were previously reviewed and approved by the FISA Court. Does that strike you as accurate?

Director MCCONNELL. Let us ask Mr. Joel.

Mr. TIERNEY. He works for you, so I am asking you. Or you didn't know this.

Director MCCONNELL. Restate the question.

Mr. TIERNEY. He says the NSA is using minimization procedures previously reviewed and approved by the FISA Court. Even though he doesn't read the PAA as requiring it, that is what is being done.

Director MCCONNELL. That is my understanding of what is being done.

The reason for that, sir, is the Court set the standard, and it has been tested in Court. It is a reasonable standard, and it is good for us to follow it.

Mr. TIERNEY. Did that in any way impede the process of implementing any of the new authorities into the PAA?

Director MCCONNELL. Not to my knowledge.

Mr. TIERNEY. Do you have an objection to requiring the FISA Court to review minimization procedures in any future FISA legislation?

Director MCCONNELL. Sir, I would be happy to take any recommendations, suggestions you have got. Remember, I tried to highlight several times, it is very complex. You want to keep asking me hypotheticals. Let us write it down——

Mr. TIERNEY. That is my point. My point is that——

Director MCCONNELL. I would be happy to look at anything you suggest, sir.

Mr. TIERNEY. This is something that your office is suggesting because they are the ones that are doing it. Mr. Joel has made the suggestion that he is carrying out the fact that he is following those previous FISA procedures and you said that didn't in any way impede the operation under the new PAA. So I assume that

you have no objection to that being written into the law. That that is what——

Director MCCONNELL. I have no objection to any recommendation that you want to make. I would be happy to examine it.

Mr. TIERNEY. Are you opposed then to the FISA Court having authority written into the law to do exactly what Mr. Joel is now doing on his own?

Director MCCONNELL. I would be happy to take the language and examine it, sir.

The point I keep trying to highlight——

Mr. TIERNEY. Do you have objection to what Mr. Joel is doing, to what he is doing now?

Director MCCONNELL. I have no objection to what he is doing now.

What I am trying to make sure everybody understands is we can't get ourselves in the situation where we were before where we are forced under a time constraint. You had a time constraint. I did not and——

Mr. TIERNEY. We have disagreement on how that time constraint came to be, and I——

Director MCCONNELL. It was your schedule, not mine.

Mr. TIERNEY. It wasn't anybody's schedule. It was a political schedule. It is a very strong point of view, and I think everybody realizes it now.

The fact of the matter is we are trying to find a way to get to a law——

Director MCCONNELL. We would be happy to look at——

Mr. TIERNEY. And apparently you now have no objection to the Court looking at those procedures for minimization and approving them.

The letter also notes that the NSA Inspector General is conducting an audit of the implementation of the new Act and that the Inspector General regularly conducts audits, inspections and reviews of compliance of minimization procedures. Why was that decision made that the NSA IG would conduct an audit in the implementation of the new Act? Do you know?

Director MCCONNELL. It has been part of the process since the beginning, to my knowledge.

Mr. TIERNEY. So I can assume you would not object to a requiring in the statute that the Inspector General makes those reviews and makes those audits in the future with respect to any civil liberties inspections. Just put into law what you are already doing.

Director MCCONNELL. Sir, I have no objection to anything you want to recommend.

Mr. TIERNEY. I am not trying to recommend. I am talking about do you have an objection to writing into law——

Director MCCONNELL. I would be happy to consider it.

Mr. TIERNEY. The function that Mr. Joel says is now happening, the Inspector General doing audits?

Director MCCONNELL. I would say again, let us write it down and let us examine.

Mr. TIERNEY. Do you have an objection to the Inspector General conducting audits?

Director MCCONNELL. I do not have an objection to the Inspector General conducting audits at the NSA. They have when I was there, and they are still there. I have no objection to that.

Mr. TIERNEY. Fine. That was very easy to get to. We didn't have to write it down.

Now, earlier, you talked about there being a large data base and so making it improbable or difficult, sometimes almost impossible, to determine the number of times that United States persons' communications were inadvertently intercepted when you were going after a target in a foreign country.

Director MCCONNELL. That is not exactly what I said.

I said we have no control over what foreign targets would talk about. Remember it is to, from, or about. So if a foreigner is talking about you and it is in the database, I may not know that. I may—could find it if I had a reason to go search for it. The database would age off in a period of time. No harm, no foul.

Mr. TIERNEY. But when somebody asks you for the number of times when a U.S. person or a person in the United States was involved in that situation, I think you said that there was some degree of difficulty in getting that done.

Director MCCONNELL. I don't know how difficult, but we will look at it and see if we can answer your questions.

Mr. TIERNEY. Would it be reasonable to have a sampling done?

Director MCCONNELL. If we can give you the total, complete answer, we will. I don't know that we can. But we will take the question and see what is doable.

Mr. TIERNEY. Thank you very much.

Thank you, Mr. Chairman.

The CHAIRMAN. Mr. Ruppersberger.

Mr. RUPPERSBERGER. We have had two hearings with you. I would like to review where I think we are.

To begin with, I think it is clear that we all agree that wiretapping foreigners to obtain critical information to protect our country is allowed under the Constitution. I think we all agree to that. Do we agree to that?

Director MCCONNELL. Foreign—say it again, sir.

Mr. RUPPERSBERGER. Wiretapping foreigners to obtain critical information——

Director MCCONNELL. What we can't allow, though, is when the wording in the bill would cause that to be in question or could be interpreted different ways.

Mr. RUPPERSBERGER. That is what we are looking for, is clarity.

And the one area I would get into, though, is I have heard this, and I want to clarify this, too. Why are you opposed to having court review procedures—this is procedures, not the individual cases—after surveillance has begun. That is a concern of mine. Not when there is an emergency situation.

Director MCCONNELL. That is what we agreed to. That is in the law.

Mr. RUPPERSBERGER. I think we are getting very close here. You know, these hearings, sometimes you wonder what you have accomplished. I think after these hearings we should be able to come together and resolve this issue.

I think the biggest area that we have is that we must have judicial oversight. Our country is a system of—we have a system of laws; and when in fact the checks and balances go the other way, we have problems, no matter who is present. And I think that what we object to is that there is not the independent judicial review, but we also understand that war against terror is a different war than we had years ago, and that is why we are attempting to resolve this.

I think we have agreed on most of the issues, other than the judicial oversight.

Now let me ask you this also, this question. The minimization issue. When in fact you have an American, where do you think the problem is that you see between certain members' point of view here and your point of view on minimization?

Mr. Wainstein.

Mr. WAINSTEIN. I am not sure exactly which members you are referring to, but I think some of us have voiced some concern that minimization isn't sufficient, that we need to get some kind of court approval before we listen in on communications appropriately intercepted against the person overseas but that are sent in to somebody in the United States.

Mr. RUPPERSBERGER. What I understand from what I am hearing and what my concern would be on the issue of minimization is that when a court—what a court does, as far as the oversight, that minimization takes the place of that. I think that is something that we can work out.

Director MCCONNELL. Frequently, what people slip into is everybody is in agreement a foreign-to-foreign communication shouldn't be an issue. But if you make that a pre-condition, what we keep attempting to highlight is you can't determine that ahead of time. So if you make a pre-condition in the law, you have effectively shut us down.

Mr. RUPPERSBERGER. From what I understand and what we are talking about today and you said that what would happen if a FISA bill didn't go forward, and I think we need to clarify that, too. We are not talking about not having a bill. We are so close on what we have negotiated, and you know that, and I know that.

Director MCCONNELL. All I am looking for is keeping the minimization process intact.

Mr. RUPPERSBERGER. If we didn't have a FISA bill, that we would be put at risk, we are not talking about that. Neither side is. What we are talking about in the one issue is that we need to have a judicial review. But we understand there are emergency situations when America is at risk when somebody is contacted; and that has to do, I think, more with operations and giving people the resources. If we need to hire more judges and hire more people in CIA, NSA to do this, we will do what we have to do.

Director MCCONNELL. And we now have judicial review. That process that Mr. Holt was making reference to about our dialogue and who we talk to, that is how the judicial review was proposed, agreed to and put in the bill.

Mr. RUPPERSBERGER. What the law basically says today, the law that was passed that we have to look at, is that, basically, under the circumstances, I don't think that you want this or we want

this, is that our government has a right to basically have the search and seizure of an American without a court order and without the Constitution being involved. We fight for liberties and freedom, and part of that——

Director MCCONNELL. I agree with that a hundred percent.

Mr. RUPPERSBERGER. So, bottom line, if you agree with that, then I am not sure where our arguments are, but we are only asking for the court to come in and review the process.

Director MCCONNELL. And that is where we are——

Mr. RUPPERSBERGER. Not even individual—that is not what it says in this law. This says that our government can have a search and seizure of American citizens.

Director MCCONNELL. No, sir. It doesn't say that at all.

Mr. RUPPERSBERGER. I disagree with that interpretation. But, if it does, then we don't have clarity, and we have to fix it, and that is our job as Members of Congress.

Mr. WAINSTEIN. If I may briefly respond to that. Just keep in mind, as the Director said, when we target surveillance on a person, a person overseas, we target against that person. If that person calls in the United States, we subject any of the information we get of the U.S. person to minimization. That is actually the only practical option.

And, in fact, that is what we do in the criminal side, too. As a prosecutor, I get a court authorization to do a title three wiretap against defendant A, he might talk to a thousand people. We don't go get court process for every one of those thousand people.

So as long as we have it against the target, we are allowed to collect and minimize that person's communications with everybody else. That is the only way this works, because otherwise——

Mr. RUPPERSBERGER. It is not that it works. We are talking about what the law says and what you can do, and it is not about who you are, you are, we are gone, somebody else comes in. We need to clarify it.

When the President comes to the district I represent and says that we need to go further than we are now, when we know—when I feel that we will be able to give you what you need to protect our country, that is where we are.

But our Constitution is what we fight for in Iraq and in World War II and the Korean war, the Vietnam war, and we have to keep focused on that. Those is our jobs.

Thank you.

The CHAIRMAN. Thank you.

The Director and Mr. Wainstein, I am told, have another hearing on the Senate side.

So Mr. Tiahrt will be the last person to have an opportunity to ask questions for 5 minutes.

Mr. Tiahrt.

Mr. TIAHRT. Thank you, and God forbid we should hold up the Senate.

Director MCCONNELL. Go ahead, sir. It is going to be an interesting hearing over there, too.

Mr. TIAHRT. I read the law before we voted on it, and I failed to see anywhere where we allowed the search and seizure of American information or any of their communications without having

some kind of a—without having the methods that you use currently. And the Protect America Act provided for the update from the 1970s law, FISA, to allow us to move into the electronic age, basically.

Director MCCONNELL. That is correct.

Mr. Tiahrt. And so now I think we are taking—it sounds to me from what we have had in our discussions this morning that we are taking scenarios that may or may not exist and hoping to write some laws to involve more lawyers and judges in the process. And, so far, I haven't found any evidence or heard of any incidents where you have violated the constitutional rights of American citizens. So I guess maybe we are extending beyond that and that we are looking at foreign citizens having the same constitutional rights that Americans have.

And I think most Americans would say that those who intend to destroy this country should not have the same rights that we have fought for and paid for in blood, and it is embodied in our Constitution.

If you follow your procedures and we are satisfied with your procedures, would you see a need for Congress to write a law for every procedure that you have that you are currently following? Is there a need for that that you see?

Director MCCONNELL. No, sir. And in my opinion, no, and my worry is what might be captured to have unintended consequences. Right now, the negotiation we had in July and early August, the Court does now review all of those procedures.

So I am satisfied that, based on our lessons learned from 1978 to the current time frame, tried and tested, our minimization process and so on, I am satisfied that it works to protect American civil liberties, and it allows us to do our mission of overseas intelligence against foreigners.

And the reason I hesitate to agree to any specific point is it could cause us to not be flexible and capable in our overseas mission if we don't say it just right. And what is in the law today works well, and I am very hesitant to agree to any changes to that.

Mr. TIAHRT. We are abiding by the Constitution with our Protect America Act, and we have judicial overview of minimization and of contacts with Americans, if they are contacted in the process of accumulating data.

Director MCCONNELL. And we have reports to this body every 6 months and, as you need to, you are welcome to look at any aspect or any part of it.

Mr. TIAHRT. Is it fair to say that today's proceedings are congressional oversight, or do you think we are avoiding our responsibility of congressional oversight?

Director MCCONNELL. No, sir. I don't think you are avoiding your responsibility. I would just like to get more of the Members to sit down and look at the data and have a feel for it, have an opportunity to meet the people that actually do this and their professionalism or commitment to also protecting civil liberties. They are very, very serious about it, so it gives you an opportunity to get some confidence in the process.

Mr. TIAHRT. I would like you to pass along to all of those you are responsible for working here in the government for, thank you for

the last 6 years of safety. No attack on our homeland. And I know there has been many, many attempts. And I am glad that we were able to update the law to move ourselves as a country into the electronic age instead of trying to proceed into the old law that was written; and I, too, am very hesitant to inject more lawyers and judicial process into the system which appears to only slow things down and makes us, in essence, less safe.

I mean, because of leaks, we have not been able to collect phone data as we have in the past before the Protect America Act. Now I think we have improved that significantly. We haven't been able to contact and follow emails as we did because of leaks in the past. We haven't been able to follow financial transactions because our allies do not cooperate back to leaks that occurred here in this country. All of those leaks I believe were intended to embarrass this Presidency, and all of them have made it more difficult for you to do your job to keep this country safe.

So, in spite of all of that difficulty in overcoming all of those obstacles, I want to thank you and the people that work for you for keeping this country safe for the last 6 months.

I yield back.

The CHAIRMAN. Thank you, Mr. Tiahrt.

And let me add my thanks for the work that you, Director McConnell and Mr. Wainstein, do for our great country. As evidenced today in our hearing, there are a variety of opinions, different concerns.

One thing that we want to do is work together to give the tools necessary to those that are in charge of keeping us safe.

So, gentlemen, thank you for being here. We appreciate your service to our Nation.

[The information follows:]

The CHAIRMAN. The hearing is adjourned.

[Whereupon, at 12:30 p.m., the committee was adjourned.]

○