FISA HEARING

HEARING

BEFORE THE

PERMANENT SELECT COMMITTEE ON INTELLIGENCE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

Hearing held in Washington, DC, September 18, 2007

U.S. GOVERNMENT PRINTING OFFICE

38–877 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

TUESDAY, SEPTEMBER 18, 2007

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

The committee met, pursuant to call, at 10:05 a.m., in room 2118, Rayburn House Office Building, the Honorable Silvestre Reyes (chairman of the committee) presiding.

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

Staff Present: Michael Delaney, Staff Director; Wyndee Parker, Deputy Staff Director/General Counsel; Jeremy Bash, Chief Counsel; Don Campbell, Professional Staff; Stacey Dixon, Professional Staff; Mieke Eoyang, Professional Staff; Eric Greenwald, Professional Staff; Robert Minehart, 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; Chris Donesa, Deputy Minority Staff Director/Chief Counsel; Frank Garcia, Minority Professional Staff; John W. Heath, Minority Professional Staff; James Lewis, Minority Professional Staff; Jamal Ware, Minority Press Secretary.

The CHAIRMAN. The committee will please come to order.

Today the committee will receive testimony from four recognized experts on the Foreign Intelligence Surveillance Act, or FISA.

Following the wire-tapping scandals of the 1970s, Congress enacted FISA in 1978 to regulate government surveillance of American citizens in national security cases. FISA instituted two important checks on the ability of the executive branch to conduct surveillance of Americans. First, the government would have to obtain an order from a specially designated court before tapping the phones of Americans on U.S. soil. Second, the government's eavesdropping activities would have to be reported to Congress.

Since 1978, much has changed. First, the threat has changed. Our focus is no longer the Soviet Union but rather a lose confederation of terrorist cells, WMD proliferators, and rogue nations.

Second, the technology has changed. Today, our calls and e-mails fly over the Internet through cell phones, BlackBerries, blogs, and chat rooms.

Third, FISA has also changed. The statute has been amended or updated by Congress in roughly 50 different ways since 1978.

And, last, Congress has made significant changes to the statute since the attacks of 9/11, including the use of John Doe roving wiretap authority, the expansion of the emergency period for obtaining court orders and authorization for targeting lone wolf suspected terrorists. Those are just a few that I wanted to mention this morning.

One thing, however, has not changed: the Fourth Amendment. It is a cornerstone of our Nation and should not be set aside, suspended or amended, not under the threat of war, insurrection, rebellion or even terrorism. To do so would greatly undermine our cherished systems of checks and balances. Our Constitution has stood the test of time. It has protected the American people for more than 200 years.

Two years ago, we were stunned to learn that, after 9/11, the Bush administration had been ignoring FISA. The NSA program involved not only targets overseas but also American citizens whose phone calls were listened to and e-mail read without a warrant. To this day, the administration refuses to share critical information about this program with Congress.

More than 3 months ago, Ranking Member Pete Hoekstra and I sent a letter to the Attorney General and to the DNI requesting copies of the President's authorizations and the DOJ legal opinions. We have yet to receive this information.

And so today I would like to say publicly to Bush's nominee for Attorney General, Judge Mukasey, one of your first tasks as Attorney General will be to repair DOJ's relationship with Congress. You can start by turning over the documents that all members of this committee have long sought relating to the NSA surveillance program.

In April, the DNI proposed some changes to FISA. The committee had planned a thorough review. In late July, in the midst of this review, the administration came rushing in with an urgent request to craft changes to FISA before the August district work period. Despite our misgivings over the rushed timing, we agreed to craft short-term legislation to ensure that our intelligence professionals had the tools that they needed to uncover plots against the U.S.

The DNI asked for three things: first, no individual warrants for foreign targets; second, a mechanism to compel the telecommunication companies to cooperate with the government, and, third, individual warrants for targets inside the United States.

We agreed to all of these things; and the leadership bill, H.R. 3356, addressed all of these issues. Further, we agreed to the DNI's request to expand this new authority from terrorism to all foreign intelligence and other changes that had been requested by the DNI.

But our administration just couldn't say yes and insisted on moving the goalposts even after striking an agreement with congressional leaders. The administration demanded its version of the legislation, even though our bill gave the Intelligence Community 100 percent of what it had asked for. The result was that Congress passed what I believe was a very flawed bill, the so-called Protect America Act.

So I want to make clear this morning our concerns are not about protecting the rights of foreign individuals overseas. The question, I believe, is when communications involve Americans, as was the case in the NSA surveillance program, what should the rules be?

I am concerned that, as drafted, the administration's bill just went too far. It allows warrantless physical searches of Americans' homes, offices and computers. It converts the FISA court into a rubber stamp, and it contains insufficient protections for Americans who will have their phone calls listened to and e-mails read under this broad new authority.

I take small comfort that the legislation sunsets in 6 months, but we will not wait. In early October, at the Speaker's request, we will mark up FISA legislation to address the needs of the Intelligence Community.

We will legislate based on the full record in this committee. We have held four hearings in June and July. Committee members and staff have made several trips to NSA to review this new authority. We have held a closed hearing on September the 6th with the NSA and FBI directors; and, after today's hearing, we will hold another open hearing on Thursday with DNI McConnell and Assistant Attorney General Kenneth Wainstein.

Our first witness today is James Baker. Mr. Baker is one of the Nation's foremost experts on FISA, having run FISA operations for the Department of Justice for the past 7 years. In 2006, Mr. Baker received the George H.W. Bush award for excellence in counterterrorism, the CIA's highest award for counterterrorism achievements. He is currently on the faculty of Harvard Law School.

Welcome, Mr. Baker.

The committee is also pleased to welcome back Mr. Jim Dempsey. He is Policy Director of the Center for Democracy and Technology. He served for 9 years as counsel to the House Judiciary Committee and remains an important adviser to Congress.

I also want to welcome Ms. Lisa Graves, Deputy Director of the Center for National Security Studies. Lisa previously served as Senior Counsel at the ACLU and as Chief Nomination's Counsel on the Judiciary Committee. She also served as Deputy Assistant Attorney General in the Department of Justice.

Welcome, Lisa.

Finally, I want to welcome David Rivkin, who is a partner at the law firm of Baker Hostetler. He has written several articles on constitutional issues. He previously served in government, at the Department of Energy and as a Special Assistant to Vice President Dan Quayle.

And now I would recognize our ranking member, Mr. Hoekstra, for any statement that he may wish to make.

Mr. HOEKSTRA. Good morning, Mr. Chairman, and good morning to the witnesses.

I have got a prepared statement which I will submit for the record. I just want to address some of the comments that the chairman made.

To characterize the notification of the U.S. Congress by the New York Times as being "stunning" and perhaps implying that that is

the first time that Congress heard about a terrorist surveillance program is inaccurate.

Mr. Chairman, I would like to submit—I don't have it with me—but to get the document and submit for the record the listing of briefings to congressional leadership by the White House on the Terrorist Surveillance Program——

The CHAIRMAN. Without objection.

[The information follows:]

Director of National Intelligence
WASHINGTON, DC 20511

MAY 17 2006

The Honorable J. Dennis Hastert
Speaker of the
House of Representatives
Washington, D.C. 20515

Dear Mr. Speaker:

I am responding on behalf of National Security Advisor Stephen Hadley to Ms. Pelosi's May 2, 2006 inquiry regarding the classification of the dates, locations, and names of members of Congress who attended briefings on the Terrorist Surveillance Program. Upon closer review of this request, it has been determined that this information can be made available in an unclassified format. The briefings typically occurred at the White House prior to December 17, 2005. After December 17, briefings occurred at the Capitol, NSA, or the White House. A copy of the list is enclosed.

Sincerely,

John D. Negroponte

Enclosure: As stated.

cc:
The Honorable Nancy Pelosi
The Honorable Jane Harman
The Honorable Peter Hoekstra
The Honorable Pat Roberts
The Honorable John D. Rockefeller IV

Event Date	Congressional Members Briefed	Name
25-Oct-01	Chair HPSCI	Porter J. Goss
	Ranking Minority Member HPSCI	Nancy Pelosi
	Chair SSCI	Bob Graham
	Vice Chair SSCI	Richard C. Shelby
14-Nov-01	Chair HPSCI	Porter J. Goss
	Ranking Minority Member HPSCI	Nancy Pelosi
	Chair SSCI	Bob Graham
	Vice Chair SSCI	Richard C. Shelby
4-Dec-01	Chair Senate Appropriations Committee, Defense Subcommittee	Daniel K. Inouye
	Ranking Minority Member Senate Appropriations Committee, Defense Subcommittee	Ted Stevens
5-Mar-02	Chair HPSCI	Porter J. Goss
	Ranking Minority Member HPSCI	Nancy Pelosi
	Vice Chair SSCI	Richard C. Shelby
10-Apr-02	Chair SSCI	Bob Graham
12-Jun-02	Chair HPSCI	Porter J. Goss
	Ranking Minority Member HPSCI	Nancy Pelosi
8-Jul-02	Chair SSCI	Bob Graham
	Ranking Minority Member SSCI	Richard C. Shelby
29-Jan-03	Chair HPSCI	Porter J. Goss
	Ranking Minority Member HPSCI	Jane Harman
	Chair SSCI	Pat Roberts
	Vice Chair SSCI	John D. "Jay" Rockefeller IV.
17-Jul-03	Chair HPSCI	Porter J. Goss
	Ranking Minority Member HPSCI	Jane Harman
	Chair SSCI	Pat Roberts
	Vice Chair SSCI	John D. "Jay" Rockefeller IV
10-Mar-04	Speaker of the House	J. Dennis Hastert
	Majority Leader of the Senate	William H. Frist
	Minority Leader of the Senate	Tom Daschle
	Minority Leader of the House	Nancy Pelosi
	Chair HPSCI	Porter J. Goss
	Ranking Minority Member HPSCI	Jane Harman
	Chair SSCI	Pat Roberts
	Vice Chair SSCI	John D. "Jay" Rockefeller IV
11-Mar-04	Majority Leader of the House	Tom DeLay
23-Sep-04	Chair HPSCI	Pete Hoekstra
3-Feb-05	Chair HPSCI	Pete Hoekstra
	Ranking Minority Member HPSCI	Jane Harman
	Chair SSCI	Pat Roberts
	Vice Chair SSCI	John D. "Jay" Rockefeller IV.
2-Mar-05	Minority Leader of the Senate	Harry Reid
14-Sep-05	Chair HPSCI	Pete Hoekstra
	Ranking Minority Member HPSCI	Jane Harman
	Chair SSCI	Pat Roberts
	Vice Chair SSCI	John D. "Jay" Rockefeller IV

Event Date	Congressional Members Briefed	Name
11-Jan-06	Speaker of the House	J. Dennis Hastert
	Majority Leader of the Senate	William H. Frist
	Chair HPSCI	Pete Hoekstra
	Chair SSCI	Pat Roberts
	Vice Chair SSCI	John D. "Jay" Rockefeller IV
20-Jan-06	Minority Leader of the Senate	Harry Reid
	Minority Leader of the House	Nancy Pelosi
	Chair SSCI	Pat Roberts
	Ranking Minority Member HPSCI	Jane Harman
11-Feb-06	Chair SSCI	Pat Roberts
16-Feb-06	Speaker of the House	J. Dennis Hastert
	Chair HPSCI	Pete Hoekstra
28-Feb-06	Chairman, House Appropriations Committee, Defense Subcommittee	C.W. Bill Young
	Ranking Minority Member, House Appropriations Committee, Defense Subcommittee	John Murtha
3-Mar-06	Vice Chair SSCI	John D. "Jay" Rockefeller IV
9-Mar-06	Chair SSCI TSP subcommittee	Pat Roberts
	Vice Chair SSCI TSP subcommittee	John D. "Jay" Rockefeller IV
	Member SSCI TSP subcommittee	Orrin G. Hatch
	Member SSCI TSP subcommittee	Mike DeWine
	Member SSCI TSP subcommittee	Dianne Feinstein
	Member SSCI TSP subcommittee	Carl Levin
	Member SSCI TSP subcommittee	Christopher S. "Kit" Bond
10-Mar-06	Member SSCI TSP subcommittee	Christopher S. "Kit" Bond
13-Mar-06	Chair SSCI TSP subcommittee	Pat Roberts
	Member SSCI TSP subcommittee	Dianne Feinstein
	Member SSCI TSP subcommittee	Orrin G. Hatch
14-Mar-06	Member SSCI TSP subcommittee	Mike DeWine
27-Mar-06	Member SSCI TSP subcommittee	Carl Levin
29-Mar-06	Chairman HPSCI TSP group	Pete Hoekstra
	Ranking Minority Member HPSCI TSP group	Jane Harman
	Member HPSCI TSP group	John McHugh
	Member HPSCI TSP group	Mike Rogers (MI)
	Member HPSCI TSP group	Mac Thornberry
	Member HPSCI TSP group	Heather Wilson
	Member HPSCI TSP group	Jo Ann Davis
	Member HPSCI TSP group	Rush Holt
	Member HPSCI TSP group	Robert E. "Bud" Cramer
	Member HPSCI TSP group	Anna G. Eshoo
	Member HPSCI TSP group	Leonard Boswell
7-Apr-06	Chairman HPSCI TSP group	Pete Hoekstra
	Member HPSCI TSP group	John McHugh
	Member HPSCI TSP group	Mike Rogers (MI)
	Member HPSCI TSP group	Mac Thornberry
	Member HPSCI TSP group	Heather Wilson
	Member HPSCI TSP group	Rush Holt
28-Apr-06	Ranking Minority Member HPSCI TSP group	Jane Harman
	Member HPSCI TSP group	Heather Wilson
	Member HPSCI TSP group	Anna G. Eshoo

Event Date	Congressional Members Briefed	Name
11-May-06	Chairman, House Appropriations Committee, Defense Subcommittee	C.W. Bill Young
	Ranking Minority Member, House Appropriations Committee, Defense Subcommittee	John Murtha

Mr. HOEKSTRA. This would also identify—or when that is put into the record will identify that congressional leadership was brought in almost immediately after 9/11 to talk about what the threat was and how best collectively Congress and the President would respond to this threat and keep America safe at a time when America was concerned about additional attacks against the United States after 9/11 because we didn't fully understand who was attacking, their capability, and what kind of sleeper cells they had.

Matter of fact, that document will show that the current Speaker of the House was briefed three times and consulted three times within the first 11 months as this program started to take shape and that the White House consulted with congressional leaders about what the program should be, the possibility and the necessity whether legislation should be done to update FISA at that time or not and how we would implement the program.

Once the program was implemented, Congress was continually briefed as to the extent of the surveillance, the types of people that were being surveilled, the protections that were being put into the process to make sure that American civil liberties were protected, the type of information that was being collected, the impact that we were having on minimizing the threats to the United States.

Let us be clear about this. This is not the Bush terrorist surveillance program. This is the Bush/congressional terrorist surveillance program. Because congressional leadership was involved in this process from the beginning.

I know when I became chairman of the committee, within the first 30 days I got the call to go over to the White House because they wanted to make sure that I was fully briefed into the program and understood exactly what the programs were and the parameters. And the last question in that meeting, in every meeting after that where I was briefed in on the program was very consistent: Do you have any concerns? Do you have any questions? Is there anything else that we need to do to address and make sure that you are comfortable with this program?

And I have to assume that for the first 3 years while this program was under way, that is exactly what happened.

And until the New York Times, in an irresponsible process and method, revealed the existence of this program, congressional leadership on the Republican and Democrat side, like I said, including the current Speaker of the House, was briefed on this program. And the reason that they went along with it for 4 years, and the parameters and under the ways that they did, was they recognized that American civil liberties were protected and they recognized that this program was having a significant impact in keeping America safe.

Republican and Democrat leadership bought into this program as being necessary, essential, and appropriate to keep America safe.

With that, I will yield back the balance of my time and submit my previous statement or the prepared statement for the record.

Thank you, Mr. Chairman.

[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 18, 2007

Good morning, and thank you to the witnesses and to the audience for coming today.

Before the August congressional recess, the House passed and the President signed urgently needed legislation to close significant and alarming intelligence gaps arising under the Foreign Intelligence Surveillance Act, or 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 been working intensely to implement the new authorities and to close the terrorist loophole, while also carefully examining how to

ensure appropriate protections for civil liberties and enhanced oversight. While a lot of work remains to be done, substantial progress has been made toward bridging the intelligence gap over the summer. Regardless of the specific authorities involved, the recent terrorism-related arrests in Germany and Denmark continued to demonstrate why timely intelligence collection is absolutely critical to our ability to thwart attacks. There should be no significant disagreement that the Protect America Act has improved our intelligence capabilities and made our country safer.

At the same time, however, I am concerned that a number of significantly inaccurate public accounts about the bill have circulated since it was passed. I am especially concerned that some of these accounts appear to be deliberate efforts to mislead and scare the American people. On this Committee, at least, we should know better. I hope that today's hearing will provide us with a full opportunity to explore these issues and to correct the many inaccuracies which have appeared in public.

One of the biggest myths that has circulated is the strained contention that the bill somehow is the product of a conspiracy to allow the government to conduct warrantless surveillance of

Americans under the cover of an effort to obtain foreign intelligence information about foreign persons. There have been repeated, clear, and explicit public statements that this is not the case.

My colleague, Congresswoman Wilson, expressly indicated her view in the Congressional Record that such "reverse targeting" is intended to be illegal under the bill. And just last week, the Justice Department firmly and publicly reiterated that FISA court orders are still required to target Americans in the United States, as they were before the new law.

It is ironic that the same people who say we have little to fear from the radical jihadists who attacked America imply that we should instead fear the hardworking, dedicated intelligence professionals we ask to defend us. Nothing could be further from the truth, and nothing in the bill reduces existing civil liberties protections, or the commitment of the civil servants in the intelligence community to be vigilant about those civil liberties.

As we consider these issues today, I hope that the Committee and the witnesses will be careful to separate facts from speculation. In the critical area of national security, we cannot set public policy based on what "might" be happening, or what "could" possibly occur.

We must be careful to understand the facts about what is happening, and intensive efforts are underway to do this across all three branches of government.

I also hope that we will continue to constructively consider the question of how to best empower the intelligence community to protect the nation. It is easy to criticize without bearing the serious and significant responsibility of protecting our nation and the American people. But this is not enough – we must also offer reasonable solutions that ensure continued vigilance while balancing civil liberties.

The Committee has already conducted extensive oversight over the implementation of the new law. Countless attorneys from throughout the Executive Branch as well as the Civil Liberties Protection Officer for the DNI have been involved in its implementation, and the procedures required by the law to protect Americans have already been submitted to the FISA Court for review well in advance of the required deadline.

Last night, I received a letter from the Civil Liberties Protection Officer for the Office of the Director of National Intelligence that details his efforts to oversee the implementation of the act and the

extensive work that is being done to protect civil liberties. I urge members to review the letter thoroughly, and I ask unanimous consent to enter the letter into the record.

So, there is certainly no shortage of lawyers involved in the consideration of these critical issues. Today's hearing, however, gives an opportunity to hear from a panel of public lawyers to hear and explore their views. I look forward to the testimony, Mr. Chairman, and to continuing the Committee's vital work to provide the Intelligence Community with all of the necessary tools to protect our nation.

The CHAIRMAN. Thank you, Mr. Hoekstra; and that is why it is imperative that we get the documents from the administration, so that we can verify the things that are true and the things that aren't true about who said what and who did what under that program.

I do remember that it was a hard issue to get the members of this committee fully read into that program. But, be that as it may, we will resolve those kinds of issues in due time, and now I want to first go down the list of the speaking order.

We are going to have Mr. Jim Baker, then followed by Mr. Jim Dempsey, Ms. Lisa Graves and then Mr. David Rivkin.

STATEMENTS OF JAMES BAKER, HARVARD LAW SCHOOL; JAMES DEMPSEY, POLICY DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY; LISA GRAVES, DEPUTY DIRECTOR, CENTER FOR NATIONAL SECURITY STUDIES; AND DAVID RIVKIN, PARTNER, BAKER HOSTETLER

The CHAIRMAN. So now I want to recognize Mr. Jim Baker; and I want to alert the members that DOJ has not cleared Mr. Baker's testimony, unfortunately, but we will, however, now have him present his oral remarks to the committee.

So, with that, Mr. Baker, you are recognized.

STATEMENT OF JAMES BAKER

Mr. BAKER. Thank you.

We have not been able to finish the clearance of the written statement, but I am able to give an oral statement today.

Mr. Chairman, members of the committee, thank you for the opportunity to come here today to discuss the Foreign Intelligence Surveillance Act and the Protect America Act. The issues that we will discuss today are complex and important and the actions that you take based upon what we talk about today will have a significant impact on the safety and the freedom of all Americans.

I would just like to make a brief statement about my background to amplify what the chairman said earlier.

From 1998 until 2007, I was responsible for intelligence operations at the Department of Justice. Working with the very dedicated men and women at the Office of Intelligence Policy and Review, we were responsible for representing the United States before the Foreign Intelligence Surveillance Court. In my time at OIPR, I reviewed, prepared, supervised the preparation of thousands of FISA applications.

The Department of Justice has specifically approved my testifying here today, but I would like to emphasize that I am appearing here in my personal capacity and that the views I express do not necessarily reflect those of the Department of Justice or the administration.

I would like to focus on three areas in my opening remarks here today:

First, I would like to talk about the productivity of the original FISA. FISA was extremely productive over the years. FISA permitted robust collection of foreign intelligence information, including actionable intelligence, and when I use the term "actionable intelligence" I mean information that the Intelligence Community

could use to take action to thwart the activities of our adversaries, including terrorist groups. We were able to disseminate information gained from FISA widely through the Intelligence Community where appropriate and to our foreign partners. We were also able to use evidence obtained from FISA in criminal prosecutions with the approval of the Attorney General.

Furthermore, everyone in the system had the comfort of knowing that their actions were clearly lawful and that they would not be subject to lawsuits or criminal prosecution for having performed in conformance with an act of Congress and Federal court order.

In many ways, it seems to me there is a paradox in that we are talking about amending Congress, and Congress amended FISA in the Protect America Act, in my view, as a result of the successes of FISA itself.

Because FISA enabled collection of vital and timely foreign intelligence information, including information about the activities of overseas terrorists, the Intelligence Community came to regard FISA as a critically important collection platform and the Intelligence Community increasingly turned to FISA to obtain important foreign intelligence information. FISA, in my view, expanded the understanding by other elements of the Intelligence Community with respect to the value of certain types of collection. That then led to a growth in the targeting of foreign operatives, which in turn then led to the desire to change the law that we were talking about today and that you were talking about in the summer.

What I would suggest is, before you decide whether to renew or modify FISA again or the Protect America Act, I would recommend asking the Intelligence Community for a thorough analysis of their assessment of the productivity of the original FISA. I believe that the record will show that FISA contributed significantly to our successes against al-Qa'ida and other terrorist groups post 9/11 and indeed that FISA worked during wartime.

That is not to say that it was easy. The very dedicated men and women of OIPR worked very long hours under sometimes very adverse conditions to enforce the laws that Congress had enacted at the time. In my view, they exemplify what it means to be a dedicated public servant, and I think their actions are worthy of the review of historians in the years to come.

A few comments about the scope of the original FISA.

To be clear, as Congress said in the legislative history, no means of collection are barred by the original statute. In other words, all forms of modern communication were and are subject to collection under the original FISA.

In addition, to clarify a point that has been discussed, FISA has never applied to foreign-to-foreign wire or radio communications. One of the problems we face today, given modern technology, is that you can't always tell where the parties are at the time of interception.

A frequent question that is also asked is whether FISA was intended to include or exclude foreign communications; and it seems to me that the analysis of that question requires a thorough understanding of several factors, including the state of technology in 1978, what Congress understood about the state of technology at that time, the lengthy and complex and somewhat contradictory at

times legislative history that exists with respect to the original FISA and, finally, a careful examination of the text of the law that Congress ultimately enacted.

With respect to the historical record, I have been looking at some documents lately just in a preliminary manner that seemed to indicate that transoceanic communications were made in relatively large quantities by both satellites and coaxial cables underneath the sea, that both kind of systems were expected to continue in service for many years and the use of fiber optics was already anticipated for undersea cables. As I suggest, the legislative history and the law can be read in a variety of ways; and it requires a careful analysis to decide what the state of play was in 1978. I suggest that if this is an important factor to you, that you task an entity such as the Congressional Research Service to do a thorough historical analysis.

Mr. Chairman, at the end of the day, the real questions regarding whether or not or how to modernize FISA ultimately are not technological in nature. It seems to me that the real questions are, number one, who should the decision maker be with respect to authorizing collection? That is, who should approve the collection before it can begin?

Second question is, what level of predication do you want to be required? That is, how much paperwork explanation is necessary to justify the collection and what standard of review should the decision maker apply?

A third question is, how particular should the approvals be? In other words, how specific must the authorizations be with respect to the persons or the facilities at which the collection is directed?

So, for example, the lower the level of approval and factual predication that is necessary and the less specific the authorizations need to be, the more quickly and more easily the Intelligence Community will be able to start collection and the greater the volume of collection they will be able to sustain over an extended period of time.

At the end of the day, that is what I believe folks are talking about when they say that we need to make the system speedy or have a system that is—provides the Intelligence Community with the speed and agility necessary to obtain the foreign intelligence they need.

A related question then is, with respect to the decision maker, what role should Federal judges play in this process? And as you can tell from the debate, this depends upon whether one or both of the targets—or the answer to that question depends on whether one or both of the targets is in the United States, whether you can actually tell where the parties who took the communication are located at the time of interception, and to what extent the government will need to review communications of the target—let me back up.

To what extent does the government need to review or find the communications of the target in order to determine where the parties to the communication are located?

Working closely with the Foreign Intelligence Surveillance Court for 10 years, I would be happy to provide the committee with the

benefit of my experience in answering that question and any other questions that the committee may have today.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Mr. Baker.

Testimony of James A. Baker

Before the

Permanent Select Committee on Intelligence

United States House of Representatives

September 18, 2007

Mr. Chairman and members of the Committee: thank you for the opportunity to appear before you today to discuss foreign intelligence collection in the 21st Century, including possible changes to the Foreign Intelligence Surveillance Act of 1978 (FISA) and the Protect America Act of 2007. The issues we will discuss today are very complex and very important. The actions you will take based upon what we are talking about today will have a significant impact on the safety and the freedom of the American people.

From 1998 until January of this year, I was responsible for, among other things, intelligence operations for the Department of Justice. Working with many dedicated professionals in my office – the Office of Intelligence Policy and Review (OIPR) – we represented the United States before the Foreign Intelligence Surveillance Court (FISC), which Congress created in 1978 under FISA. I have prepared, reviewed, or supervised the review and preparation of thousands of FISA applications. The Department of Justice has specifically approved my testifying before the Committee today. Let me emphasize, however, that I am appearing here strictly in my personal capacity, and that the views I express do not necessarily reflect those of the Department of Justice or the Administration.

In the brief time that I have available this morning, I would like to focus on three areas that I think are important to understand in order to determine how best to conduct foreign intelligence collection today. I will not discuss the threat that we face today from hostile foreign powers such as international terrorist groups like al Qaeda. Based upon information that the Intelligence Community has made available to the public, it seems to me that we should assume that we face significant threats that will persist for some time. It appears that al Qaeda wishes to cause as much death and destruction as possible with respect to the United States, and is actively seeking to acquire the means to do so.

FISA's Productivity. First, FISA collection has been extremely productive over the years. The version of FISA that was in effect until August of this year enabled the Intelligence Community to obtain timely and accurate foreign intelligence information about the capabilities, plans, intentions, and activities of foreign powers, persons, organizations, and their agents. FISA served us well throughout the Cold War and it continued to serve us well after the fall of the Soviet Union, even post-9/11. Until the Protect America Act passed in August of this year, most of the core definitions and procedures of FISA had not changed since 1978. And yet using FISA we were able to collect a significant amount of actionable foreign intelligence information (meaning that the Intelligence Community could take prompt action on it) to thwart the plans and activities of our adversaries, including terrorist groups. We could also disseminate the information appropriately within the government and to our foreign partners, and use the information acquired as evidence in criminal trials with the approval of the Attorney General. At the same time, everyone in the system had the comfort of knowing that their actions were lawful, and that they would not be subject to lawsuits or criminal

prosecution for having performed in conformance with an act of Congress and federal court orders.

Indeed, there is a paradox with respect to the entire discussion that we are having today. The calls for FISA to be amended result ultimately from the success of FISA itself. Because we were able to collect vital intelligence information in a timely manner through FISA – especially including information about the activities of terrorists located overseas – the Intelligence Community came to regard FISA as a critically important collection platform. U.S. intelligence agencies increasingly turned to the FISA process to obtain the information that they needed to execute their duties. Moreover, I also believe that our success in FISA collection informed elements of the Intelligence Community about the value of certain types of collection, which led to the growth in the targeting of foreign operatives that has resulted in the desire to change the law that we see today.

Before you decide whether to renew or modify the Protect America Act or make other changes to FISA, I believe that you should ask the Intelligence Community for a thorough analysis of the productivity of the FISA program. I have testified previously before this Committee in closed session about those successes, which I am unable to repeat here today in open session. Suffice it to say that I believe that the record will show that the original FISA contributed significantly to our successes against al Qaeda and other terrorist groups post-9/11, and that FISA worked during wartime. That is not to say that it has been easy. The dedicated men and women from the Office of Intelligence Policy and Review who worked long hours under adverse conditions to enforce the law that Congress had enacted deserve the Nation's gratitude. Each of them exemplifies what

it means to be a dedicated public servant. And their actions are worthy of the examination of historians in the years to come.

FISA's Scope. Second, let me focus for just a moment on what we can collect under FISA. To begin with, no means of collection are barred by the 1978 statute. We could obtain authorization to collect all forms of modern communication under the original FISA. Let's also clarify another point – FISA has never applied to wire or radio communications that are clearly from one person in a foreign country to another person in a foreign country. As I discuss a bit later, the problem we face today is that it is not always easy or possible to tell where all of the parties to a communication are located when the interception takes place. Further, one of FISA's definitions of electronic surveillance covers monitoring of stored electronic communications in the United States regardless of the location of the communicants. FISA also covers physical searches in the United States, including searches of residences and stored data, and other collection as well.

Much has been made in the recent past about what types of communications Congress intended to cover in the original FISA and what it sought to exempt. While it is important to understand what Congress intended when it enacted FISA in 1978, I am not sure that it is determinative of what we should do today. In any event, in order to fully understand the role that technical issues played in the legal and policy decisions of the time, one must consider several factors: (1) the historical record to determine what the state of technology was in 1978 and what technological advances were foreseen or reasonably foreseeable at that time; (2) what Congress understood in 1978 about the state

of technology; (3) what Congress intended to cover with the law that it enacted; and (4) what the law that Congress enacted actually covers.

With respect to the state of technology at the time, my preliminary review of some public record materials that I have accessed only recently seems to indicate that transoceanic communications were made in relatively large quantities by both satellites (radio) and coaxial cables (wire); that both kinds of systems were expected to continue in service for many years; and that the use of fiber optics was already anticipated for undersea cables. The lengthy and complex legislative history shows that Congress was concerned about, and considered, many factors when enacting FISA, and some parts of the legislative history appear to suggest that it may well have intended to exclude international communications from the scope of the Act (although this conclusion may be undercut by the fact that at least one of the definitions of electronic surveillance on its face includes international communications, a point on which the pertinent legislative history concurs). If you believe today that it is important to analyze the historical record and the full legislative history in order to inform your decision on pending legislation, I strongly recommend that you ask entities such as the Congressional Research Service (CRS) to conduct a thorough review of all available materials and provide you with their conclusions.

In my view, the real questions regarding whether or not (or how) to modernize FISA ultimately are not technological in nature. Instead, the real questions are: (1) who should be the decision-maker (that is, who should approve foreign intelligence collection before it can begin); (2) what level of predication should be required (that is, how much paperwork and explanation is necessary to justify such collection and what standard of

review should apply); and (3) how particular should the approvals be (that is, how specific must the authorizations be with respect to the persons or facilities at which the collection is directed). The lower the level of approval and factual predication needed, and the less specific the approvals are, the more quickly and more easily the Intelligence Community can start collection, and the great the volume of collection it can sustain over extended periods. That, I believe, is what is meant when one says we need to achieve greater speed and agility in foreign intelligence collection. All of this leads me to my next point.

Role of the Court in Intelligence Collection. As others have discussed, such as David Kris, co-author of the recently published *National Security Investigations and Prosecutions*, one of the key questions with respect to foreign intelligence collection that faces us today is when, and under what circumstances and conditions, should the government be allowed to conduct electronic surveillance (and search) for long periods of time without individualized findings of probable cause made in advance by judges. The Constitution does not mandate that judges play any role in foreign intelligence collection, so long as the collection activities are otherwise reasonable. But it seems to me that there is general consensus today that the FISA court should approve electronic surveillance and physical search in advance when those collection activities are targeted at people who are clearly located inside the United States. This includes surveillance of all domestic-to-domestic communications. Similarly, there appears to be consensus that the court should play no role in approving collection when the surveillance is targeted at people who are clearly located outside the United States, even when the collection itself takes place

inside the United States. As I mentioned previously, foreign-to-foreign wire or radio communications traditionally have fallen outside the scope of FISA.

There appears to be less agreement in two other areas. The first is where one end of the communication is, or may be, in the United States, and the other end of the communication is outside the United States. This is sometimes referred to as "one end U.S. communications." The second is where you cannot tell in advance (if ever) where one or both of the parties to a communication are located. This is a particular issue with Internet communications, including web-based email, as well as mobile telephone technology.

Contrary to what some have said, the privacy interests of Americans may be implicated in these situations. When the government targets a foreign national who is abroad, the Fourth Amendment may be implicated if the electronic surveillance results in the interception of communications of a United States person. It may be implicated if the government acquires and listens to (or stores and later examines) a communication to which a United States person is a party, and it may be implicated if the government intercepts and scans the content of such a communication in order to determine whether it is to, from, or concerning a foreign national target who is located abroad.

Whenever the Fourth Amendment is implicated, the government's collection activities must be reasonable. The determination of whether particular collection activities are reasonable will likely depend on many factors, including: (1) as noted above, when and under what circumstances and conditions, the government is allowed to conduct electronic surveillance (and search) for long periods of time without individualized findings of probable cause made in advance by judges; and (2) the

adequacy of any minimization procedures that are in place to limit the acquisition, retention, and dissemination of irrelevant information concerning United States persons.

Having worked closely with the FISA court for more than 10 years, I would be happy to provide the Committee with the benefit of my experience as it endeavors to determine the appropriate role for federal judges in approving and reviewing foreign intelligence collection in the two scenarios I have discussed.

Thank you.

The CHAIRMAN. Now, Mr. Dempsey, you are recognized for your opening statement.

STATEMENT OF JAMES DEMPSEY

Mr. DEMPSEY. Mr. Chairman, Ranking Member, members of the committee, good morning. Thank you for the opportunity to testify at this hearing.

The issue before the committee today has nothing to do with terrorism suspects overseas talking to other people overseas. For a long time, there has been agreement among Members of Congress of both parties and even in the civil liberties community that a court order should not be required for interception of foreign-to-foreign communications. Instead, the debate over the past year has been about the rights of American citizens and others inside the United States when they are talking to people overseas.

Of course, the NSA needs speed and agility collecting communications of persons overseas; and many of those persons overseas will communicate only with other overseas persons, not affecting the rights of Americans at all.

However, it is also certain that some of those persons overseas will communicate with people in the United States. Some percentage, maybe a growing percentage, of NSA's activities directed at persons overseas result in the acquisition and dissemination and use of communications to and from the U.S.

Individuals in the U.S. retain their reasonable expectation of privacy in their communications even when they are communicating with people overseas. When the government listens to both ends of the communication, it infringes on the privacy rights of Americans.

The administration would like us to think of this as just two issues: targeting people in the U.S., warrant required; targeting people overseas, warrant not required.

I think there is a third category as well, which is when the government is targeting no one particular person at all and we have the NSA sifting and sorting and collecting communications to and from the United States.

And minimization means not what we think it might mean. Minimization allows the government to use, collect, retain, share, and rely upon those communications of U.S. citizens.

Mr. Chairman, I prepared a much longer memo on minimization and, with your permission and consent with the committee, I would like to enter that into the record.

The CHAIRMAN. Without objection.

[The information follows:]

CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

Minimization Cannot Be Relied Upon to Protect the Rights of Americans under a Warrantless Surveillance Program

September 17, 2007

"Minimization" is the Administration's one word answer to concerns that the rights of American citizens will be infringed by the warrantless surveillance authority approved by Congress before its August recess in the "Protect America Act" (PAA).

Reliance on "minimization" to defend the PAA fails for two reasons:

(1) Even if "minimization" meant that the government discarded all intercepted communications of Americans – which it does not – it would not cure the damage done to privacy when the communications are intercepted in the first place. The police cannot come into your house without a warrant, look around, copy your files and then claim no constitutional violation because they threw everything away after they looked at it back at the station house.

(2) Under FISA, "minimization" does not mean that the government must discard all of the communications of people in the US "incidentally" collected when the government is targeting someone overseas. To the contrary, the "minimization" rules that would be applicable to the PAA permit the government to retain, analyze, and disseminate to other agencies the communications of people inside the US, including US citizens.

Under the "minimization" rules applicable to the PAA, the American citizen talking to relatives in Lebanon, the charities coordinator planning an assistance program for Pakistan, the businessman trading with partners in the Middle East, or the journalist gathering information about the opium trade in Afghanistan – all while sitting in the US – might have their international calls or emails monitored, recorded and disseminated without judicial approval or oversight if the NSA, in its sole discretion, decided to "target" the person they were talking to overseas.

Summary

There are two very different kinds of "minimization" under FISA. The version that applies to the surveillance authorized under the Protect America Act does not require the NSA to discard or mask all information concerning Americans that is collected when the

government is targeting foreigners. See 50 U.S.C. §1801(h)(1) – (3). **To the contrary, "minimization" gives the NSA authority to collect, retain and disseminate certain communications to which a US citizen is a party.** Anything that is foreign intelligence or evidence of crime can be retained and disseminated. Under the PAA, the NSA has the sole discretion to decide what is foreign intelligence; it has sole discretion to decide what to collect, keep and disseminate, with no judicial oversight of any stage of the process. This kind of minimization offers inadequate protection to the rights of Americans whose calls will inevitably be intercepted under the PAA without judicial approval.

A key point must be stressed: This permissive type of minimization applicable to the PAA was intended under the original FISA to operate in conjunction with a warrant, as an additional protection, not to be a substitute for a warrant. Under traditional FISA, the court approved both the initial search and the minimization procedures, and the court retained jurisdiction over the implementation of the minimization rules. Under the PAA, in contrast to most of FISA, no judge approves either the search or the minimization rules.

There is another, very different type of minimization under FISA, applicable only to a narrow sub-category of surveillance, namely the warrantless surveillance of leased lines used by foreign embassies under circumstances where it is highly unlikely that the communications of Americans will be intercepted. 50 U.S.C. §1801(h)(4). This type of minimization requires the government to promptly discard any communications to which a US person is a party or to obtain a FISA court order to retain and use them. It should be noted that the Administration is urging Congress to repeal this kind of minimization in its broader FISA "reform" bill.

This second, protective type of minimization was specifically intended to apply to warrantless surveillance, but it does not apply to warrantless surveillance under the PAA. Even if this protective type of minimization were applied to the PAA, it could not substitute for court approval of such a broad and ill-defined range of surveillance as that contemplated under the PAA.

In sum, the minimization procedures applicable to the PAA do not provide protection for the rights of Americans.

Background – The Focus of Privacy Concern in the Current Debate Is the International Communications of US Persons – That Is, Communications with One Party in the US

It has long been clear that the debate over FISA this year has not been about terrorism suspects overseas talking to other people overseas. Both Democrats and Republicans were agreed on addressing that problem by making it clear that FISA did not apply to interception of foreign-to-foreign electronic communications even if the surveillance occurred on US soil. (As a result of developments in global communications networks,

calls and Internet communications from one foreign location to another may pass through switching facilities in the US.)

Instead, the debate for the past year has been over the rights of American citizens and others inside the US, where the Constitution's special protections apply. The NSA repeatedly stresses that it wants to target persons overseas, but it is undeniably certain that some of those persons overseas will communicate with people in the US. The individuals in the US retain their reasonable expectation of privacy in their communications, including their communications with persons overseas. The government will "listen" to both ends of the communication, infringing on the privacy rights of the Americans.

Thus, the program at the center of the debate – a program legitimately intended to provide speed and agility to the NSA in targeting persons overseas, but certain to infringe on the privacy of some Americans – poses two questions: (1) how does the government decide who might be a terrorist overseas, and (2) what happens when the target overseas communicates with someone in the US?

The Administration's stock answer to both questions is that it "minimizes" the communications of the person inside the US. As we will show, minimization does not mean that the government must destroy all communications of Americans. To the contrary, minimization rules allow the government to retain and disseminate certain communications of citizens and other U.S. persons.

But no definition of minimization could answer the first question: Is the surveillance program reasonably calibrated to intercept communications of terrorists overseas (or others overseas with foreign intelligence information)? When surveillance will intrude on the privacy of persons inside the United States, the question of how to target that surveillance is one our democratic system generally commits to prior judicial review. It should be a judge who decides in the first place that the government's filtering and selection methods are reasonably designed to intercept the communications of terrorists and are not likely to unnecessarily intercept the communications of innocent Americans.[1] The question of what communications to intercept cannot be resolved by administrative procedures that limit the use of the information once it is collected.

Nor would we want an overly rigid rule limiting use of communications between persons overseas and persons in the US. The second question, which is what to do with the communications of Americans that will inevitably be intercepted, cannot be answered by a blanket rule that the NSA must ignore all those communications. If a terrorist overseas is talking to a person in the US, that might be precisely the kind of communications that

---

[1] The PAA submits the wrong question to judicial review. The PAA requires the Administration to submit to the court procedures for ensuring that the persons being targeted are outside the U.S. The question that should be reviewed by the court is whether the targeting procedures reasonably ensure that the communications being targeted will contain foreign intelligence.

we would want the NSA to keep and to disseminate to the FBI, DHS and other law enforcement and intelligence agencies. Minimization rules ***should*** allow the retention and use of some communications of Americans. That is why some independent (although not necessarily particularized) review of targeting practices is necessary upfront, and it is also why oversight of minimization practices is necessary. Picking and choosing which communications of Americans to retain and which to discard should not be left to the sole discretion of the Executive Branch. Just as the police in carrying out an ordinary search must make a return of service –that is, police must report back to the judge after the search on how they conducted the search and what they seized – so the minimization decisions of the NSA must be subject to judicial oversight.

The NSA has entered a new era. During the Cold War, the NSA had a philosophy – not actually required by law or applied in practice, but a strongly held philosophy nevertheless – that it would have nothing to do with US person data. That philosophy has been abandoned.[2] The NSA is collecting, and finding intelligence value in, a lot more communications to and from the US persons than ever before. A reasonable set of checks and balances needs to be developed for this new era. The PAA provides for none.

The Statutory Definition of Minimization

Warrantless surveillance authorized under the Protect America Act is subject to minimization procedures that meet the definition of "minimization procedures" in section 101(h) of FISA. 50 U.S.C. §1801(h). That definition states:

> (h) ``Minimization procedures", with respect to electronic surveillance, means--
>
> > (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
> >
> > (2) procedures that require that nonpublicly available

[2] In its "Transition 2001" report, completed in December 2000, the NSA concluded, "The National Security Agency is prepared organizationally, intellectually and--with sufficient investment--technologically, to exploit in an unprecedented way the explosion in global communications. This represents an Agency very different from the one we inherited from the Cold War. It also demands a policy recognition that the NSA will be a legal but also a powerful and permanent presence on a global telecommunications infrastructure where protected American communications and targeted adversary communications will coexist."

> information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
>
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
>
> (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

Of the four numbered paragraphs of the definition, two are restrictive, one is permissive and one applies only to surveillance pursuant to the "embassy exception." The restrictive provisions are subject to exceptions, so the overall effect of the definition is to permit the government to collect, retain and disseminate certain communications of American citizens and other US. persons.

Paragraph (1) requires the Attorney General to adopt "procedures that minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons." This restriction is limited, however, for the procedures must be "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." In other words, the NSA can acquire, retain and disseminate to other agencies information about US persons if it constitutes "foreign intelligence information."

The FISA definition of "foreign intelligence information" is broad. It includes not only information concerning potential attacks by foreign nations or international terrorists, but also "information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to -- (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States." 50 U.S.C. §1801(e)(2).

A lot could hinge on the interpretation of what is "necessary," but there is no public definition in statute, case law or Administration guideline as to what is "necessary." Under the PAA, since the FISA court has no supervisory role over the warrantless

surveillance of international calls, the determination of what is "foreign intelligence" and what is "necessary" is left to the NSA.

Paragraph (2) of the definition of "minimization procedures" requires the NSA to redact the identity of a U.S. person before disseminating information "which is ***not*** foreign intelligence information, as defined in subsection (e)(1)" of the FISA definitions (emphasis added). This is pretty convoluted, but it apparently permits the NSA to disseminate the identity of US persons in connection with information that ***is*** foreign intelligence under (e)(1), which is the prong of the definition of foreign intelligence information that relates to international terrorism. In other words, if the information ***is*** foreign intelligence under (e)(1), paragraph (2) provides no protection to the U.S. person. Also, paragraph (2) clearly permits NSA to disseminate **any** intelligence concerning US persons so long as it redacts the identity of the U.S. person. General Hayden described the redaction process in his 2005 confirmation hearing:

> ... it is not uncommon for us to come across information to, from or about what we would call a protected person--a U.S. person. ... The rule of thumb in almost all cases is that you minimize it, and you simply refer to ``named U.S. person'' or ``named U.S. official'' in the report that goes out. http://www.fas.org/irp/congress/2005_hr/shrg109-270.pdf p. 20.

So minimization doesn't mean that NSA has to purge the identity of the US person from its files. The information remains in storage along with the identifying information, which is available for later search and retrieval. Officials at other agencies can request the names of U.S. persons that were redacted from NSA reports. *Newsweek* reported in May 2006 that between January 2004 and May 2006, the agency had supplied the names of some *10,000* American citizens to various interested officials in other agencies.[3]

Finally, paragraph (2) permits the NSA to disseminate identifying information about a US person when it is "necessary to understand foreign intelligence information or assess its importance." It has been reported that, after 9/11, the head of the NSA changed internal interpretations of the redaction procedures to allow routine dissemination of identifying information about US persons, presumably on the ground that information identifying U.S. persons was necessary for the FBI and other agencies to follow-up on the intelligence.[4] Indeed, under the NSA's new practice, the FBI was flooded with

---

[3] http://www.msnbc.msn.com/id/7614681/site/newsweek/. The practice came to light most recently when U.N. ambassador nominee John Bolton explained to a Senate confirmation hearing that he had requested that the names of U.S persons be unmasked from NSA intercepts on 10 occasions when he was at the State Department.

[4] Eric Lichtblau and Scott Shane, "Files Say Agency Initiated Growth of Spying Effort." *New York Times*, January 4, 2006. In the context of court-authorized surveillance, this may have been appropriate. For a discussion of the dissemination of identifying information, see the recommendation on "authorized use" in the Third Report of the Markle Task Force on National Security in the Information Age. It is unclear whether the

information identifying U.S. persons.[5]

Paragraph (3) of the minimization definition allows the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed, with all identifiers intact.

Paragraph (4) is the only provision that requires the government to delete communications to which a person is a party within 72 hours. This applies only to communications intercepted under FISA's leased line exception (sometimes called the "embassy exception"). It is inapplicable to surveillance authorized by the PAA.

It is important to note that the Administration's broader FISA "reform" bill, which it promises to push this fall, would repeal paragraph (4). See Administration April 2007 proposal, page 4 of 66 http://www.cdt.org/security/nsa/Bush2007FISAbill.pdf. In other words, the Administration would repeal the only provision of FISA that actually requires it to discard communications of US persons.[6]

Suzanne Spaulding, former Minority Staff Director for the House Intelligence Committee and former Assistant General Counsel at CIA, argued in her September 5 testimony to the House Judiciary Committee that the protective type of minimization in paragraph (4) should be extended to the PAA. However, even the strictest form of minimization would not be a substitute for prior court approval in light of how broad and ill-defined is the range of surveillance contemplated under the PAA (and Spaulding did not suggest otherwise). Moreover, while it was expected that the "embassy exception" would almost never result in the interception of the communications of Americans, it *is* expected that the surveillance authorized by the PAA will sweep in a number of international communications to which an American is a party. Almost certainly, some of these foreign-to-domestic communications will contain foreign intelligence. Because it will be much more frequently necessary to decide which U.S. person communications to retain and which to discard, any minimization rules applicable to the surveillance of communications between people overseas and people in the US should be subject to judicial approval and monitoring. Yet the PAA denies the FISA court the power to review the minimization rules for the program or monitor their application. The Reyes-

---

Administration intends to apply these same liberal dissemination rules to information acquired under the PAA, which is likely to result in an increase in the collection of information identifying US persons.

[5] Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta Jr, "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," *New York Times* (January 17, 2006).

[6] The Administration bill would also vastly expand the scope of the so-called embassy exception, *id.* at pp. 5-6, so that the government could, without a warrant, intercept, retain and disseminate many more domestic-to-domestic calls, including calls to, from and between citizens in the US.

Rockefeller bill presented a workable approach for judicial approval and ongoing judicial oversight of surveillance programs that will likely intercept communications with US persons can be found in the Reyes-Rockefeller draft.

In sum, the FISA definition of "minimization" permits the NSA to collect, retain and disseminate throughout the government any information extracted from the communications of US citizens that the NSA believes is foreign intelligence or evidence of a crime. Under the PAA, that judgment is left solely to the discretion of the NSA. There are no checks and balances against NSA mistakes.

USSID 18

Further detail about minimization is found in United States Signals Intelligence Directive 18. This is a major document prescribing policies and procedures for conducting signals intelligence activities affecting the US persons. A redacted, declassified version of USSID 18 issued in 1993, by DNI McConnell when he was Director of NSA, is online at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-01.htm. There may have been amendments since then, but it is probably safe to assume that they are no more restrictive (privacy protective) than the 1993 version.

There is no requirement that USSID 18 apply to surveillance under the PAA. However, the guideline reaffirms that minimization permits the retention and dissemination of communications of Americans inadvertently collected when targeting persons overseas.[7]

One of the more interesting provisions of USSID 18 is Section 6, which describes the circumstances in which communications to, from, or about US persons can be retained. The authority specifically permits retention of communications in databases for "traffic analysis":

> Except as otherwise provided in Annex A, Appendix 1, Section 4, communications to, from or about U.S. PERSONS that are intercepted by the USSS may be retained in their original or transcribed form only as follows:
>
> (1) Unenciphered communications not thought to contain secret meaning may be retained for five years unless the DDO determines in writing that retention for longer periods is required to respond to authorized FOREIGN INTELLIGENCE requirements.
> (2) Communications necessary to maintain technical data bases for cryptanalytic or traffic analysis purposes may be retained for a period

[7] USSID 18 and its Annexes contain revealing, and not always intuitive, definitions of "collection," "interception," and "acquisition" that may give the NSA quite broad discretion to record international communications for later processing.

> sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future FOREIGN INTELLIGENCE requirement. ... If a U.S. PERSON'S identity is not necessary to maintaining technical data bases, it should be deleted or replaced by a generic name when practicable.

Congress should look into the current scope of these NSA "technical data bases."[8]

Minimization Must Be Measured Against Something, Butt the PAA is Without Standards

Minimization is part of the constitutional essence of a reasonable search. It is the way that the government complies with the fundamental requirement that a search must be confined to the grounds that justified it in the first place. If a search is pursuant to a warrant, the scope of the search must be limited to that specified in the warrant. If a search is conducted without a warrant, "[t]he scope of the search must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible." Terry v. Ohio, 392 U.S. 1, 17 (1968). In United States v. Ross, the Supreme Court said, "The scope of a warrantless search ... is defined by the object of the search and the place in which there is probable cause to believe that it may be found." 456 U.S. 798, 820 (1982). *See also* Horton v. California, 496 U.S. 128, 139 (1990) ("a warrantless search [must] be circumscribed by the exigencies which justify its initiation").

Minimization, therefore, must relate to something – there must be some parameters for the search against which minimization can be measured. One of the reasons why the PAA is almost certainly unconstitutional is because it authorizes searches inside the US with no criteria other than "the acquisition of foreign intelligence concerning persons reasonably believed to be outside the United States." Even if one were to accept the argument that a court order is not be required in some cases for national security searches, it seems highly unlikely that a warrantless search program intruding on the communications privacy of Americans could be justified solely on the ground that the surveillance was intended to collect foreign intelligence concerning persons overseas with no guidance on how to identify those persons and communications. Looking at every international communication as a way of finding foreign intelligence is a blanket search.

---

[8] Under Section 5 of the FISA court minimization procedures appended to USSID 18, even domestic communications that are reasonably believed to contain technical data base information may be disseminated to the FBI and to other elements of the U.S. SIGINT system.

Minimization Is Not a Substitute for Judicial Approval

One of the seminal wiretap cases, Katz v. US, 389 U.S. 347 (1967), made it clear that minimization does not make a warrantless search constitutional. In Katz, the government agents had probable cause. They limited their surveillance in scope and duration to the specific purpose of establishing the contents of the target's unlawful communications. They took great care to overhear only the conversations of the target himself. On the single occasion when the statements of another person were inadvertently intercepted, the agents refrained from listening to them. None of this saved the surveillance constitutionally. The Supreme Court said:

> It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized. In the absence of such safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end. Searches conducted without warrants have been held unlawful "notwithstanding facts unquestionably showing probable cause," Agnello v. United States, 269 U.S. 20, 33 , for the Constitution requires "that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police . . . ." Wong Sun v. United States, 371 U.S. 471, 481 -482. "Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes," United States v. Jeffers, 342 U.S. 48, 51 . . . . [389 U.S. at 356 – 357]

Conclusion

In many ways, minimization is reminiscent of "the Wall" – a widely misunderstood rule, rigidly but unevenly applied, that does not well serve either national security or civil liberties.

The effort to define workable, truly protective minimization rules cannot be abandoned. Minimization is part of the constitutional reasonableness standard, which provides the rock-bottom minimum for all government searches infringing upon a privacy interest. Minimization is also desirable operationally: in some ways, it is part of the selection and filtering process of separating relevant from irrelevant information that is the heart of the intelligence process.

We do not question the good faith of NSA employees, who have always taken pride in their scrupulous approach to U.S person data. However, these employees operate under tremendous pressure. In the new age of terror, minimization committed to the NSA's discretion cannot be relied upon to fully protect the rights of Americans. The factors impinging on NSA's work include:

- The targets are poorly defined: Given the fragmented, decentralized nature of the terrorist threat, the government often may not have precise targeting criteria. If we are looking for needles in a haystack, we don't even have a good idea of what a needle looks like anymore. As a result, the government feels compelled to intercepts and analyzes a lot of communications whose intelligence significance is uncertain.
- The haystack is enormous: The blessing and the curse of the digital revolution is that there is so much information readily available to the government.
- The threshold for action has been lowered: Given the risk of catastrophic attack, information about ambiguous and in fact innocent matters will be disseminated and acted upon and individuals will suffer consequences of mistaken inferences.

In this environment, the NSA is acquiring and disseminating significantly larger quantities of conversations to which a U.S person is a party, and it is more likely that the NSA is analyzing and disseminating information about seemingly relevant but in fact innocent behavior. As more information about citizens and other U.S persons is being relied upon to make decisions directly affecting individuals, checks and balances are needed at each step of the process.

The terrorist watch list is a perfect example of how this new intelligence environment can affect ordinary Americans. The watch list now contains over 700,000 entries, created on the basis of reports from a range of intelligence agencies. The list is growing at the rate of 20,000 entries a month. A recent study by the Department of Justice Inspector General found that, even after vetting by the Terrorist Screening Center, 38% of the records on the list contained errors or inconsistencies. In 20% of the cases that have been resolved where members of the public complained that they were inappropriately lists, the complaint was resolved by entirely removing the name from the watchlist. The list, however, is secret. Individuals must guess as to whether they are on it in order to seek redress.[9] The list is used not only as the basis for the passenger screening program that affects 1.8 million air travelers a day. The watchlist feeds into the Violent Gang and Terrorist Organization File, which is made available through the NCIC to over 60,000 state and local criminal justice agencies and may be relied upon by police in ordinary encounters with citizens on a daily basis.

---

[9] Ellen Nakashima, "Terrorism Watch List Is Faulted For Errors," Washington Post September 7, 2007 at p. A12. The IG report is at http://www.usdoj.gov/oig/reports/FBI/a0741/final.pdf.

In this environment, we need lots of checks and balances. Minimization is part of that. But minimization is not enough, constitutionally or practically. And minimization defined and applied solely at the discretion of the Executive Branch is clearly not enough.

For more information, contact Jim Dempsey (202) 365-8026 or Greg Nojeim (202) 637-9800 x 113.

Mr. DEMPSEY. Now how do we normally protect and overcome a person's privacy interest? Of all of the millions of calls to and from the United States, how do we ensure that the government's interception activity is not careless or misguided or based on unreasonable assumptions?

The answer under our Constitution, normally, is we require a court order for that decision. It is the court order that protects and overcomes the privacy interests of persons on both ends of the call. When a judge issues a court order, she knows she is authorizing the government to infringe on the privacy of people on both ends of the communication. The warrant approves the interference with the privacy of both the target, so to speak, and all other persons on that targeted facility or communications channel.

Even if one party has no fourth amendment rights, the other parties to the communication retain theirs; and it is the court order that is necessary to protect the interest of those persons, in this case the persons in the United States.

The Protect America Act is completely without standards in this regard. It does not require that the person overseas be suspected of being an agent of a foreign power. It doesn't require that the NSA have probable cause or any reasonable suspicion of anything except that the person be outside the United States.

There is no limit on the scope or duration of the surveillance. There is no court approval of the minimization rules. There is no court supervision of how the calls of Americans are being treated, how they are being used.

We can give the NSA the speed and agility it needs, while at the same time protecting rights of Americans. We can do that through a two-step process: A blanket order or program order—a basket order sometimes it is called—authorizing a program of electronic surveillance inside the United States intended to intercept the communications of persons overseas, plus a process for determining when individualized orders are necessary because the surveillance has shifted or the center of gravity has begun to interfere significantly with the rights of people in the United States.

The court granting the initial blanket order would not have to approve and should not approve the specific targeting decisions. But by creating jurisdiction in the court and, by the way, giving the companies which we want to compel to cooperate the certainty of a court order and then creating the jurisdiction in the court to supervise and to review the periodic reports back to the court about how the surveillance is being carried out, I think we can strike the right balance here, provide the intelligence agencies with the speed and agility that they need and, at the same time, protect the rights of the Americans on the American end of these communications.

Mr. Chairman, I would be happy to answer your questions and those of the other members of the committee. There are, obviously, a host of issues that we need to go through here. One could dig in on the question of exclusivity, the question of immunity for service providers, a host of other issues; and I look forward to questions on those issues.

The CHAIRMAN. Thank you.

[The statement of Mr. Dempsey follows:]

Statement of James X. Dempsey
Policy Director
Center for Democracy & Technology*

before the
House Permanent Select Committee on Intelligence

Foreign Intelligence Surveillance Act (FISA) and NSA Activities

September 18, 2007

Chairman Reyes, Ranking Member Hoekstra, and Members of the Committee, thank you for the opportunity to testify this morning.

The Director of National Intelligence has laid out three basic requirements for FISA legislation:

- No particularized orders for surveillance designed to intercept the communications of foreigners overseas.
- A court order for surveillance of Americans.
- Immunity for service providers that cooperate with the government.

All three of these goals can be achieved in a way that serves both the national security and civil liberties, guided by the principles of operational agility, privacy and accountability. The Protect America Act, adopted last month under intense pressure, fails to achieve the Administration's stated requirements in a rational and balanced way. We will outline here how to achieve the Administration's goals within a reasonable system of checks and balances, suited both to changes in technology and the national security threats facing our nation.

I. No Particularized Orders for Surveillance Designed to Intercept the Communications of Foreigners Overseas

A. The Debate Concerns Communications To and From People in the US

The debate over FISA this year has not been about terrorism suspects overseas talking to other people overseas. For a long time, there has been agreement among Members of Congress in both parties, and even in the civil liberties community, that a court order

---

* The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the new digital communications media. Among our priorities is preserving the balance between security and freedom after 9/11. CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies and associations interested in information privacy and security.

should not be required for interception of foreign-to-foreign communications even if the surveillance occurs on US soil. To achieve balanced resolution of this sometimes heated debate, we should put aside any generalized rhetoric about surveillance of terrorists abroad. That is not the issue.

Instead, the debate for the past year has been over the rights of American citizens and others inside the US, where the Constitution's protections apply even to national security activities. The NSA argues that it is only "targeting" foreigners overseas, but it is certain that that some of those persons overseas will communicate with people in the US. When the government intercepts communications of citizens and others inside the US, it is interfering with the privacy of those persons inside the US, even if the government is "targeting" persons overseas.

The NSA argues, with justification, that its needs agility and speed when targeting persons overseas and should not need to prepare applications for particularized orders for foreign targets overseas when the interception of those communications may not interfere with the rights of anyone in the US. It seems likely that a certain percentage of foreign intelligence targets overseas will communicate only with other foreigners overseas, so it seems reasonable to assume that a certain percentage of surveillance targeted at persons overseas will not affect the rights of people in the US. Furthermore, the NSA argues that it cannot be sure in advance whether a particular targeted person overseas will sometime in the future have a communication with someone in the US.

However, it is also certain that some of those persons of interest to NSA overseas will communicate with people in the US. Some percentage – most likely a growing percentage – of NSA's activities targeted at persons overseas result in the acquisition of communications to and from the US.[1] The individuals in the US retain their reasonable expectation of privacy in their communications even when they are communicating with persons overseas. When the government "listens" to both ends of the communication – as it admits it will do in some cases – it infringes on the privacy rights of the Americans.

When surveillance will intrude on the privacy of persons inside the United States, the question of how to conduct that surveillance – what facilities (places) to search and what communications (things) to seize -- is one our Constitution generally commits to prior

---

[1] In his 2005 confirmation hearing, General Hayden said "it is not uncommon for us to come across information to, from or about what we would call a protected person--a U.S. person." http://www.fas.org/irp/congress/2005_hr/shrg109-270.pdf p. 20. In its "Transition 2001" report, completed in December 2000, the NSA concluded, "The National Security Agency is prepared ... to exploit in an unprecedented way the explosion in global communications. This represents an Agency very different from the one we inherited from the Cold War. It also demands a policy recognition that the NSA will be a legal but also a powerful and permanent presence on a global telecommunications infrastructure *where protected American communications and targeted adversary communications will coexist*." (Emphasis added.)

judicial review. It should be a judge who decides in the first place that the government's activities are reasonably designed to intercept the communications of terrorists or other foreigners overseas likely to contain foreign intelligence and are not likely to unnecessarily intercept the communications of innocent Americans.

B. Searches Without a Warrant Are Presumptively Unconstitutional

All searches, even national security searches, are subject to the Fourth Amendment. They must meet the reasonableness standard. In order to be reasonable, searches must be based on particularized suspicion, they must be limited in scope and duration and, with rare exceptions, they must be conducted pursuant to a warrant.

Several courts have held that a warrant is not required for particularized searches to collect foreign intelligence where there is reason to believe that the subject of the search is an agent of a foreign power engaged in espionage or terrorism. The Supreme Court has never ruled on the issue and it must be considered unresolved. However, no court has ever permitted warrantless searches as broad and standardless as those authorized under the PAA. For example, while *US v Butenko*, 494 F.2d 593 (3rd Cir. 1974), held that a warrant is not required for foreign intelligence surveillance, it went on to emphasize that, even in national security cases, "The foundation of any determination of reasonableness, the crucial test of legality under the Fourth Amendment, is the probable cause standard." 494 F.2d at 606. Likewise, in *US v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980), the Fourth Circuit held that "the government should be relieved of seeking a warrant only when the object of the search or the surveillance is a foreign power, its agent or collaborators."

The PAA falls far short of the standards enunciated in *Butenko* and *Truong*. It is not limited to searches of the communications of foreign powers or agents of foreign powers. Searches under the PAA are not based on probable cause. They are not reasonably limited in duration.

Given the utter lack of standards, it is highly likely that a search under the PAA of the international communications of US persons would be unconstitutional. If a search is conducted without a warrant, "[t]he scope of the search must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible." *Terry v. Ohio*, 392 U.S. 1, 17 (1968). The PAA does not set forth any limits tied to any special circumstances, other than the generalized need to collect any foreign intelligence.

C. The PAA Provides Inadequate Judicial Review of Surveillance Activities Likely to Affect the Rights of Americans

DNI McConnell has accepted the principle of judicial review[2] and the PAA has a procedure for FISA court review of certain procedures, but it is woefully inadequate and does not provide assurance of the Act's constitutionality:

- The PAA submits the wrong question to judicial review. The PAA requires the Administration to submit to the FISA court procedures for ensuring that the persons being targeted are outside the U.S. We have no doubt that the NSA will target persons overseas. The question that should be reviewed is whether, in choosing among all the foreigners overseas, NSA uses procedures reasonably designed to identify and collect the communications of those whose communications may have foreign intelligence value. This would seem to be the minimum standard for national security surveillance. Such a limitation may be imposed on the NSA by Section 105B or E.O. 12333, but given the Fourth Amendment implications of electronic surveillance, it should be judicially enforced.
- The PAA sets a standard of review – "clearly erroneous" – that is too low. The clearly erroneous standard is used by appellate courts to review trial court findings of fact, and it is appropriate for the Executive Branch's determination under FISA that information is foreign intelligence. It is entirely unsuited to ex parte review of the threshold search and seizure standards involving the protection of Fourth Amendment rights.
- The review provided in the PAA comes too late – after the surveillance has begun. That may have been considered necessary when the Administration claimed that there was a crisis and that surveillance needed to start immediately in order to prevent an attack during August. Now that the government is operating under the PAA, it has time to define and refine its targeting and filtering criteria so that they can be submitted to the FISA court for prior judicial review.
- The review under the PAA does not result in a court order authorizing surveillance and compelling corporate cooperation. In fact, under the PAA, it appears there would be no consequences were the FISA court to declare the Administration's targeting procedures to be inadequate.

---

[2] "I could agree to a procedure that provides for court review -- after needed collection has begun -- of our procedures for gathering foreign intelligence through classified methods directed at foreigners located overseas. While I would strongly prefer not to engage in such a process, I am prepared to take these additional steps to keep the confidence of Members of Congress and the American people that our processes have been subject to court review and approval." Statement by Director of National Intelligence, Subject: Modernization of the Foreign Intelligence Surveillance Act (FISA), August 2, 2007 http://www.cdt.org/security/nsa/dnistm82.pdf.

After-the-fact minimization of seized communications cannot take the place of judicial review of the decision of where to search in the first place. Because the minimization rules undoubtedly (and justifiably) will allow the retention and use of some communications of Americans captured under a program "targeting" foreigners overseas, some independent (although not necessarily particularized) review of targeting practices is necessary upfront.

D. A More Effective and Balanced Approach

It is possible to balance the Administration's argument that a particularized court order is not feasible for interception activities targeted at persons overseas against the need to ensure that the government's activities do not unnecessarily or broadly infringe on the communications privacy of persons inside the US.

At the very least, the FISA court should review whether the government's selection and filtering methods are reasonably likely to ensure that (1) the communications to be intercepted are to or from non-US persons overseas and (2) such communications contain foreign intelligence. The second prong of this standard affords the government wider latitude than the "agent of a foreign power" standard. It should be made clear that the court cannot review the specific selectors (for example, specific phone numbers) or filters, but rather reviews the criteria for determining those selectors and filters.

A court order authorizing a program of surveillance directed at persons overseas has three major advantages:

- It creates jurisdiction in the FISA court for oversight of the implementation of the program, the application of the minimization rules, and the process for seeking an order when the surveillance begins to infringe significantly on the rights of people in the US.
- It provides the communications companies the certainty they deserve if they are expected to cooperate with wiretapping. Reliance on Attorney General certifications leaves corporations unsure of their liability.
- It is more likely to be constitutional. The PAA authorizes a program of warrantless surveillance far broader than anything approved by any court. It is very risky for the government to be proceeding with a program of national security significance whose constitutionality is highly debated. The purpose of FISA was to place national security surveillance on a firm constitutional footing. If the NSA's surveillance does disclose a terrorist threat inside the US, the government should have the strongest constitutional basis for using information acquired under the program to carry out arrests or further domestic surveillance.

II. A Court Order for Surveillance of Americans

A. "Targeting" Is Not the Standard for Assessing Fourth Amendment Rights

The Administration agrees that the surveillance of Americans should be subject to a regular order under FISA. But the Administration argues that a court order is needed only when it is "targeting" a US person in the US, and that it should be able to intercept the communications of American citizens and other US persons so long as it is not "targeting" the US person. For constitutional purposes, "targeting" is not the relevant question. Indeed, in 1978 (after FISA was enacted), the Supreme Court rejected the concept of "targeting" as the basis for evaluating Fourth Amendment rights. *Rakas v. Illinois*, 439 U.S. 128 (1978). Instead, Fourth Amendment rights turn on whether a person has a reasonable expectation of privacy and whether that expectation was infringed upon. Persons in the US clearly have a reasonable expectation of privacy in their communications, and the government infringes on that right when it intercepts those communications. *Katz v. United States*, 389 U.S. 347 (1967) and *Berger v. New York*, 388 U.S. 41 (1967).

It makes no difference to the rights of Americans that the people overseas they are communicating with have no Fourth Amendment right. In a recent case, the Supreme Court held that when two people share a space and one of those persons waives her Fourth Amendment rights, the second person does not lose his. A search taken over the objection of the second party, the Supreme Court held, is unconstitutional even though the other party no longer had a Fourth Amendment right. *Georgia v. Randolph*, 547 U.S. ___ (2006).

B. Minimization Is Not Sufficient to Protect the Rights of Americans

CDT has prepared and will submit for the record a lengthy analysis on "minimization." Our analysis shows that reliance on "minimization" to defend the PAA fails for two reasons:

(1) Even if "minimization" meant that the government discarded all intercepted communications of Americans, it would not cure the damage done to privacy when the communications are intercepted in the first place. The police cannot come into your house without a warrant, look around, copy your files and then claim no constitutional violation because they threw everything away after they looked at it back at the station house.

(2) Under FISA, "minimization" does not mean that the government must discard all of the communications of people in the US "incidentally" collected when the government is targeting someone overseas. **To the contrary, the "minimization" that would be applicable to the PAA permits the government to retain, analyze, and disseminate to other agencies the communications of US citizens.**

Under the "minimization" rules applicable to the PAA, the American citizen talking to relatives in Lebanon, the charities coordinator planning an assistance program for rural areas of Pakistan, the businessman buying or selling products in the Middle East, or the journalist gathering information about the opium trade in Afghanistan– all while sitting in the US – might have their international calls or emails monitored, recorded and disseminated without judicial approval or oversight.

One of the seminal wiretap cases, *Katz v. US*, 389 U.S. 347 (1967), made it clear that minimization does not make a warrantless search constitutional. In Katz, the government agents had probable cause. They limited their surveillance in scope and duration to the specific purpose of establishing the contents of the target's unlawful communications. They took great care to overhear only the conversations of the target himself. On the single occasion when the statements of another person were inadvertently intercepted, the agents refrained from listening to them. None of this saved the surveillance constitutionally. The Supreme Court said:

> It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized. In the absence of such safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end. Searches conducted without warrants have been held unlawful "notwithstanding facts unquestionably showing probable cause," Agnello v. United States, 269 U.S. 20, 33, for the Constitution requires "that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police . . . ." Wong Sun v. United States, 371 U.S. 471, 481 -482. "Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes," United States v. Jeffers, 342 U.S. 48, 51 . . . . [389 U.S. at 356 – 357]

C. A More Effective and Balanced Approach

There needs to be a mechanism for addressing those situations where the communications of an American are intercepted as a result of activities designed to intercept the communications of persons reasonably believed to be overseas. Minimization can help address this problem, but, as *Katz* held, minimization without a court order does not make a search constitutional.

Minimization may be sufficient to address the truly incidental collection of the communications of persons inside the US. However, when the surveillance of the communications of an American becomes significant, particularized court review should be triggered. The development of a standard for particularized review should take into account the fact that the NSA generally does not analyze communications in real time and does not analyze all of the communications it intercepts. The best approach may be through the use of periodic reports to the FISA court under the program warrant we recommended in section I. Such periodic reports about the results of blanket searches targeted at the communications of persons overseas would allow the court to identify when certain surveillance activity is significantly infringing on the rights of Americans.

III. Communications Companies Deserve Immunity for Cooperation with Lawful Interception, Not for Assisting in Unlawful Surveillance

A. The Responsibilities of Communications Service Providers

Under our nation's electronic surveillance laws, communications service providers have a dual responsibility: to assist government surveillance and to protect the privacy of their subscribers. Without the service providers' cooperation with *lawful* surveillance requests, it would be much more difficult for the government to listen in when terrorists communicate. Without the carriers' resistance to *unlawful* surveillance requests, the privacy of innocent Americans' communications would be threatened by zealous officials acting on their own perception, rather the law's definition, of what is right and wrong.

Accordingly, FISA created -- and Congress should preserve -- a system of incentives for corporate assistance with *lawful* surveillance requests and disincentives for assistance with *unlawful* requests. This system includes immunity and compensation for expenses when cooperating with lawful surveillance and damages liability when carriers conduct unlawful surveillance.

B. Retroactive Immunity Would Undermine the Structure of FISA

DNI McConnell has implied that companies that cooperated with the so-called Terrorist Surveillance Program violated FISA and are therefore exposed to ruinous liability. He has called on Congress to retroactively immunize the companies.

In many respects, the question of retroactive immunity is premature. Congress could safely do nothing on this issue. The cases against the companies are dealing with procedural issues and it will be several years before there is a judgment on the merits.

More importantly, retroactive immunity would be inconsistent with the structure and purpose of FISA. FISA was intended to provide clarity to both communications companies and government officials. Retroactive immunity would undermine the role the communications carriers play in effectively checking unlawful surveillance. It would place all carriers in an impossible position during the next crisis. If the government

approached them with a request for surveillance that did not meet the statutory requirements, they would be uncertain as to whether they should cooperate in the hope that they would later get immunity. A communications service provider should not have to guess whether cooperation with an apparently illegal request will be excused.

Liability for unlawful surveillance is crucial to the exclusivity of FISA. If the carriers who cooperated with the unlawful aspects of the TSP are forgiven for violating the law, then FISA becomes optional, for every time in the future that an Attorney General asks service providers to cooperate with surveillance not permitted by FISA, they may do so in the hope and expectation that they will provided immunity if found out.

To reinforce the exclusivity of FISA, the immunity provisions of FISA and Title III should be clarified to condition communications service provider immunity on receipt of either a court order or a certification from the Attorney General that the surveillance meets a statutory exception specified in the certification.

C. A More Effective and Balanced Approach to Immunity

Retroactive liability is necessary for the FISA system to function properly in the future. But ruinous liability is not. Under FISA, any person other than a foreign power or an agent of a foreign power who has been subjected to unlawful electronic surveillance is entitled to recover at least liquidated damages of $1,000 or $100/day for each day of violation, whichever is greater. 50 U.S.C. Section 1810. If the conduct of the TSP was illegal, it could have affected millions of Americans, resulting in very large aggregate damages. The simplest and fairest solution would be to impose a cap on damages. However, until the facts about this warrantless surveillance program are publicly known, we urge Congress to defer any action in response to the request for immunity. Congress should not retroactively change the rules on conduct that has not been fully explained to it or to the public.

D. Security and Privacy Concerns with the Technology of Compliance

There are enormous risks in the technical details of how communications service providers cooperate with government surveillance. In the absence of legislative guidance, the government and communications service providers are likely to conduct secret discussions to make compliance easy for both the companies and the government. This may entail installation of special software or hardware in service provider switching and storage facilities or other changes in communications networks. Congress cannot ignore this aspect of FISA, however it is amended. As computer security experts have noted, changes to communications networks intended to facilitate government interception can have unintended impact on privacy and security.[3]

---

[3] Susan Landau, "A Gateway for Hackers: The Security Threat in the New Wiretapping Law," *Washington Post*, August 9, 2007, p. A17 http://www.washingtonpost.com/wp-dyn/content/article/2007/08/08/AR2007080801961.html.

E. Additional Elements of Accountability

In recent years, there have been numerous problems with the Executive Branch's implementation of intelligence gathering powers. A number of these problems came to light only as a result of Inspector General audits. Earlier this year, for example, a Congressionally-mandated study by the DOJ Inspector General documented misuses of the National Security Letter authority. The report laid out problems that the Attorney General had previously denied existed, even after he had been internally informed of them.

Congress should heed these lessons and include in any FISA legislation a charge to the appropriate Inspectors General to conduct periodic audits to measure the extent to which communications with persons in the United States are being intercepted without a particularized court order, and to assess whether the government is properly seeking a FISA court order when activities targeted at persons overseas are infringing on the rights of Americans. The Inspector General audit could also assess the adequacy of NSA's selection and filtering techniques, to determine how often surveillance targets reasonably believed to be abroad turn out to be in the United States.

The results of the audit should be reported to the House and Senate Intelligence and Judiciary Committees.

IV. The PAA May Authorize Warrantless Acquisition of a Wide Range of Stored Communications

It is impossible to tell whether the PAA is very cleverly drafted or very carelessly drafted. In truth, it is probably some of both. It is clear that the statute is subject to multiple interpretations. There has been considerable debate about whether it encompasses various privacy intrusions – physical searches, access to business records, interception of domestic-to-domestic communications -- going beyond communications surveillance of international communications.

This concern grows out of the decision to base the PAA around a provision that says, in Alice-in-Wonderland fashion, that certain forms of electronic surveillance are not "electronic surveillance," thereby upsetting a very complex statute that contains many authorities and restrictions keyed to the definition of "electronic surveillance." It is compounded by the unwise use at the beginning of Section 105B of the phrase "Notwithstanding any other law. … ." It also is compounded by the inconsistent use of undefined terms like "directed at" and "concerning."

The Administration has sought to dampen these fears, but it is apparent that the PAA does not establish clear rules for intelligence activities that the Administration says are of utmost importance to the national security. The goal of FISA was to provide certainty to intelligence agency personnel working under pressure. The PAA undermines that goal.

In at least one respect, it does appear that the PAA – intentionally or unintentionally -- authorizes a new form of government access to communications, including possibly domestic-to-domestic communications. This new authority concerns access to stored communications.

When FISA was enacted, almost all electronic communications were ephemeral: if they were not captured in real time, they were gone. Among the many consequences of the digital revolution and the rise of the Internet is something CDT calls the "storage revolution." Huge quantities of our email are stored on the computers of service providers, often for very long periods of time. With the advent of voice over IP services, the storage of voice communications may also become more common. See CDT's report "Digital Search & Seizure" (February 2006) http://www.cdt.org/publications/digital-search-and-seizure.pdf.

Stored communications are covered by the Stored Communications Act, part of the Electronic Communications Privacy Act of 1986. It is unclear how stored communications fit within the FISA framework. FISA's definition of electronic surveillance is limited to the acquisition of communications "by an electronic, mechanical, or other surveillance device." If an email service provider accesses the stored communications of its subscriber, copies them and sends them to the government, is that the use of "an electronic, mechanical, or other surveillance device?" If it is not, then the acquisition of those stored communications is not electronic surveillance. And if something is not electronic surveillance, then the powers of Section 105B are available.

Section 105B added by the PAA creates a powerful mechanism for the government to force communications service providers (and maybe others) to cooperate with the government's acquisition of stored communications without court approval. Section 105B expressly applies to communications "either as they are transmitted or while they are stored" and to "equipment" that is being used to store communications. While Section 105A exempts from FISA any surveillance that is *directed at* targets believed to be abroad, Section 105B empowers the Attorney General, without a warrant, to compel service providers to cooperate with the acquisition of foreign intelligence information *concerning* persons believed to be abroad. Section 105B applies not only to communications exempted from FISA by virtue of Section 105A, but to other means of "acquisition" of communications that are not electronic surveillance. Information may "concern" a person abroad even if it is in the communications of a US person. Probably every email from the New York Times Baghdad bureau to editors in New York contains foreign intelligence concerning persons outside the US. If the disclosure of email by a service provider is not "electronic surveillance," then the PAA creates a major new authority. The language that introduces Section 105B – "Notwithstanding any other law" – would seem to override the stored communications act or any other law on access to stored email.

At the very least, this is an issue to be explored and clarified.

Conclusion

In the new environment of global communications networks, and in light of the threat of borderless terrorism, it is likely that the NSA is acquiring and disseminating significantly larger quantities of conversations to which a US person is a party. As more information about citizens and other US persons is being relied upon to make decisions directly affecting individuals, checks and balances are needed at each step of the process. The legitimate goal of providing the NSA with speed and agility in targeting persons overseas can be accomplished in a way that builds on the constitutional system of judicial review. The Center for Democracy and Technology looks forward to working with the Committee to achieve that objective.

The CHAIRMAN. Now Ms. Graves, you are recognized.

STATEMENT OF LISA GRAVES

Ms. GRAVES. On behalf of the Center for National Security Studies, I want to thank the chairman and the ranking member for having this hearing today, for having the privilege to testify on FISA and the PAA. We appreciate very much your scheduling this hearing in public so quickly in the aftermath of the temporary revisions that were passed in August.

We believe that the far-reaching changes written into FISA are unconstitutional and they are unnecessary because there are alternatives that provide additional flexibility to the Intelligence Community and increase its effectiveness while preserving Americans' constitutional rights and the checks and balances. But every reasonable alternative was unreasonably rejected and the breadth of the PAA is, in a word, breathtaking. We fear that the PAA authorizes too much surveillance among Americans and fails to provide the kind of independent, individualized checks that are essential to protect civil liberties, and the requirements permitted by the PAA will undoubtedly sweep in increasing numbers of American communications with no independent protection for their rights.

We need clear rules. There needs to be flexibility. But these rules are ambiguous and elastic; and history demonstrates that political leaders will, specially in times of fear, unilaterally and secretly read even narrow authorizations broadly. It is not clear exactly what kind of searches, whether electronic or physical, the PAA might allow. The kind of who, what, where, when, how often, how long required under FISA are missing under the PAA.

It seems quite clear, however, that the intent was to eliminate the search warrant requirement for a substantial number of American communications.

As Jim said, this is not about foreign-to-foreign communications, and I think as Mr. Baker said as well. And, in fact, the administration has taken this position publicly in various settings. But this isn't about the Terrorist Surveillance Program. It is not about al-Qa'ida calling the U.S. It is not limited to terrorists. It is not limited to weapons of mass destruction proliferators. What it is about is getting access to the networks and nodes in the United States that involve the international calls and e-mails of Americans and foreigners.

And what it changes dramatically is the access to those calls from the fiber optic networks here in the United States without a warrant, and doing that required a warrant until last month and for the last 30 years. The PAA eliminates that protection.

I think it is important to remember the history of FISA in this regard, and I understand from Mr. Baker there has been a lot of talk back and forth about that history. But let me just explore for a moment one key point regarding Operation Shamrock.

As the members of this committee know well, Congress intended to prohibit the NSA from restarting Operation Shamrock, which was an operation that had been in effect for decades in which the NSA obtained the electromagnetic tapes of nearly all telegrams going into and out of the United States to analyze them for foreign

intelligence information, for information to protect national security.

When FISA was passed in 1801(f)(2), Congress barred acquisition—not targeting—acquisition of communications off the wires of the United States. That protection is eliminated plainly by this law.

Now there are some who will say that the case law before FISA was passed was ambiguous or perhaps some courts had not ruled that such action was unconstitutional. But let me add a note about your power as Congress and your role, in my opinion.

The courts in this area of national security are particularly weak in intervening when the executive branch asserts national security interests. Under the political question doctrine or other doctrines, they are hesitant to intercede; and the administration urges them not to.

And the executive branch is not the sole organ, is not the best protector of individual liberties in this regard. It was Congress's role. It was a necessity for Congress to make this judgment, and Congress made a judgment that the Constitution required there to be a warrant before the Intelligence Community has access to the telecommunications cables going into and out of the United States for Americans' international communications.

That was a correct judgment then, and it is a correct judgment to this day.

Now the administration claims that there are some times when they don't know who is calling into the United States, whether it is a foreigner or not. But it seems to us that the packet technology, the technology that makes a call actually go from point A to point B, that makes it reach its destination, includes information that relatively quickly someone can ascertain who the originator is and who the target is or who the caller is and who the recipient is.

We think that in a large number of communications you can know where those communications are going or we wouldn't receive calls or e-mails that we do, which we do most of the time.

They also assert that there are some number of communications where they don't know where a call is coming from or where an e-mail is going to. But this is not a justification to sweep in all communications where they do know and can know particularly where American communications are involved.

We think that it is critically important that this committee take a very hard look at the effect of the PAA, both the intended consequences and the unintended consequences. Because we believe this bill allows access to the facilities in the United States without any court oversight or meaningful oversight by the courts without any individual checks before the fact or after the fact, and basically it entrusts the Intelligence Community to take what they choose without any independent oversight.

We fully support your efforts to get full disclosure of all of the documents you have requested, and we would request that significant amounts of those be made public to the extent possible. We believe it is essential for this committee to have a detailed report of the number of Americans who have been subject to surveillance without warrants already in the last 45 days.

We believe that individualized court orders are essential and also you need mandatory oversight. Apparently, optional oversight doesn't work, as you can't get documents you have been already seeking for months.

We think it is critically important that you obtain the legal opinions and the court orders. And we believe that there has been ambiguity, to say the least, about the description of this program, as demonstrated by the statements by Chairman Rockefeller and former Ranking Member Harman of this committee.

And let me just conclude on two points: First, there has been a tremendous globalization of American communications over the last 30 years. Forty million Americans travel abroad every year. A half a million Americans work abroad or serve in the military abroad. A couple of million Americans live overseas. A quarter of a million students study abroad a year. And all of these Americans, and Americans here, are in closer contact than ever with friends, family and business associates abroad.

We need adequate and perhaps increased protections for Americans in these circumstances.

The networks that will be accessed through the blanket orders that are presumed under this Act are networks that contain all American communications and some foreign communications, all American communications.

Second, Americans' rights should not be reduced to the same as those people without constitutional rights. It shouldn't go to the lowest common denominator of the foreigner on the call. The Americans still retain those rights. And, as we have said before, we believe that minimization is inadequate and constitutionally problematic as a policy matter to protect the privacy of Americans.

In conclusion, the Center for National Security Studies believes that 30 years ago Congress made the right judgment with more information before it than any court has ever had before it about what happens when there isn't a judicial check, and we would ask you to restore these protections and appropriate flexibility for the protection of our national security and for the protection of our constitutional rights.

Thank you.

The CHAIRMAN. Thank you, Ms. Graves.

[The statement of Ms. Graves follows:]

"The Foreign Intelligence Surveillance Act and Effectively Protecting the Liberty and Security of Americans"

Testimony of
Kate Martin and Lisa Graves
Center for National Security Studies
Washington, DC

Before the House Permanent Select Committee on Intelligence
United States House of Representatives
September 18, 2007

On behalf of the Center for National Security Studies and my partner there, Director Kate Martin, I thank Chairman Reyes and the Ranking Member for the privilege of testifying before this Committee today on the Foreign Intelligence Surveillance Act (FISA), effective intelligence and protecting the civil liberties of Americans. We appreciate your scheduling this public hearing so quickly in the aftermath of the temporary revision of FISA that was passed in haste in August.

We believe that the far-reaching changes written into FISA are unconstitutional. They are unnecessary because there are alternatives that would provide additional flexibility to the intelligence community and increase its effectiveness while preserving Americans' constitutional rights, and constitutional checks and balances. Nevertheless, every reasonable alternative—more funding for FISA procedures, streamlining rules for court review, additional time to seek warrants after-the-fact in emergencies, rules to clarify that purely foreign-to-foreign communications that transit the US do not require a warrant, and provisions to allow for the commencement of surveillance before it is known whether Americans' communications will be intercepted—was unreasonably rejected. We hope Congress will reverse course this fall.

The Center for National Security Studies was founded in 1974 to ensure that civil liberties are not eroded in the name of national security, just as Congress began a period of robust oversight of the secret, unchecked intelligence gathering that had violated the rights of hundreds of thousands of Americans. The Center is guided by the conviction that our national security must and can be protected without undermining the fundamental rights of individuals guaranteed by the Bill of Rights. In our work, we begin with the premise that both national security interests and civil liberties protections must be taken seriously and that by doing so, solutions to apparent conflicts can often be found without compromising either.

The Center was called to testify before Congress when FISA was first considered. FISA itself was the product of over two years of legislative drafting and thorough consideration, word by word, to establish clear rules to better protect the rights of Americans and ensure that intelligence gathering was properly focused. Since then, the Center has been asked to testify many times concerning FISA, and we have filed numerous amicus briefs and lawsuits concerning the lawfulness of FISA and related procedures.

We applaud this Committee's insistence on this public debate about FISA and the Protect America Act (PAA). It is essential to the proper functioning of our constitutional democracy, and the complaint that it is harmful is, at its heart, a claim for unreviewed and unchecked presidential power to conduct secret surveillance of Americans.

The PAA amendments authorize unconstitutional surveillance of Americans.

The amendments enacted in August authorize a dramatic increase in secret surveillance of Americans in violation of the Fourth Amendment's requirements for a judicial warrant based on individualized probable cause. As described below, the amendments authorize the NSA and other government agencies to seize massive volumes of telephone and e-mail communications to and from individuals and Americans located in the United States from communications facilities in the United States. The PAA authorizes such seizures without:

- ✓ Any judicial warrant;
- ✓ Any finding of probable cause by any court or even by the Attorney General; or
- ✓ Any requirement that any court or even the Attorney General specify
  - o the persons whose communications will be seized,
  - o the location of such seizures, or
  - o the method or means of such seizures.

Individualized review of such activities by an independent court is the fundamental safeguard for protecting the civil liberties of Americans. The orders the administration has authorized itself to write could well be blanket orders, the kind of "general warrants" the Founding Fathers sought to prevent in the Fourth Amendment, which commands that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

When Congress passed FISA in 1978, it recognized that adherence to these Fourth Amendment requirements is necessary to protect against the kind of abuses that had occurred for many years before then. It specifically required a FISA warrant for the acquisition of electronic communications in the United States of international or domestic communications to or from United States persons. The PAA eliminated this constitutionally required protection in the FISA. Congress should restore those Fourth Amendment protections for individual privacy.

A sea change—broad expansion of warrantless access to Americans' calls and e-mails.

Although the administration initially said it was having difficulty obtaining access to terrorists' foreign-to-foreign communications that transit the US, the PAA authorizes warrantless acquisition of vastly more communications than simply those among foreign terrorists or even other foreign nationals abroad.

It is important to remember that even the surveillance authorized by court order under FISA is an extraordinary and extremely instrusive prower. FISA confers extraordinary authority on the government, namely to wiretap Americans in secret and never notify them that the government has obtained tapes of all their conversations and copies of all their e-mails. Congress approved such authority in 1978, on the stipulation that there would be individualized determinations of probable cause made by a judge before such secret surveillance could be undertaken. When the constitutionality of such secret searches was challenged (by individuals who had been notified of the wiretapping because they had been indicted), FISA was upheld because of the protections it contained. The PAA eliminates many of these constitutionally required safeguards in the FISA.

We fear that the PAA authorizes too much secret surveillance involving Americans and fails to provide the kind of independent, individualized checks that are essential to protect civil liberties. The breadth of the statute's exemptions from FISA's warrant requirements is extremely troubling. While we have respect the professionalism of NSA linguists, analysts, and technicians who work to protect our nation, their jobs are to collect against requirements. And the requirements permitted by the PAA will undoubtedly sweep in increasing numbers of American communications, with no independent protections for their rights. Moreover, history has demonstrated that political leaders will—especially in times of fear such as this period following the tragic attacks of 9/11—unilaterally and secretly read even narrow authorizations broadly.

The broad language appears to authorize some physical searches without warrants.

For example, it is very unclear what effect the PAA has on the Executive's authority to conduct secret physical searches inside the United States. The plain language of the law written by the administration is so broad that it permits the "acquisition" (seizure) of "information" (electronic communications or stored communications) "concerning" (about) a person located outside the US (a person, company, or group). In addition, the PAA contains express language allowing the Executive to unilaterally "extinguish" any "electronic surveillance or physical search" orders of the FISA court that were in effect when the law was passed while giving broad authority to obtain information in secret through searches of stored records.

While it is not clear what such secret searches (whether physical or electronic) might entail—the kind of who, what, where, how and how often or long required by FISA but not the PAA—it seems clear that the intent was to eliminate the requirement for a search warrant in at least some circumstances. The Congress needs a clear understanding of that intent and any court orders extinguished or modified pursuant to the PAA. Certainly no public justification has been offered to eliminate or weaken any of the requirements for physical searches in the US. Assurances aside, the breadth of the language is very troubling.

The PAA sweeps much more broadly than the controversial TSP activities.

We would also note that the PAA authorizes much broader warrantless surveillance of Americans than the surveillance described as the "Terrorist Surveillance Program." There is no requirement that PAA's surveillance involve foreign terrorists and those suspected of conspiring with them. There is not even any requirement that the purpose of such warrantless surveillance be to obtain information related to terrorism. Time and again, the administration deliberately

insisted on broad language over clearer language with defined parameters. The law must be clear and there must be real judicial oversight to protect individual rights—we must be governed by the rule of law, not the whims or even good intentions of political or career appointees.

The PAA appears to authorize access without warrants to all international communications of Americans, whenever the surveillance is "directed at" a person, group, corporation, foreign political party or government outside the US.

We do not believe there is any serious dispute that the administration's intent in the PAA was to allow the warrantless interception of any communication with at least one foreign terminal or leg. But neither terminal is required to be a foreign terrorist. The potential reach is sweeping. It appears to allow the warrantless interception of any communication involving any person located outside the US—a definition that covers roughly potentially millions of people, thousands of corporations, and hundreds of groups—and their communications with any one of 300 million people in the US, including countless corporations and groups, so long as gathering foreign intelligence is the objective.

When confronted with this interpretation, the administration has responded that they could not possibly process *all* international calls and e-mails of Americans, not that they would not have greatly expanded access to them. We have asked whether they will "sit on the wire" monitoring communications flowing through US telephone and internet companies and use technology to acquire and analyze digital calls and e-mails to or from Americans without warrants, and there is no straight answer.[1]

So, to determine what kind of surveillance is now authorized, the first two sections of the PAA must be read together with the sections of FISA containing the definitions. Section 1 of the PAA exempts from FISA's warrant requirements and other protections any "surveillance directed at a person reasonably believed to be located overseas" by exempting such surveillance from the definition of "electronic surveillance," which is the trigger for FISA's warrant requirements. This change alone does not "clarify" the intent of FISA to exempt foreign to foreign communications even if seized in the United States. Instead, it fundamentally weakens FISA by drastically limiting the requirement to obtain a warrant for "the acquisition . . . of the contents of any wire communication to or from a person in the United States . . . if such acquisition occurs in the United States." The PAA thus eliminates the FISA warrant requirement for international communications by Americans, whenever such acquisition is carried out as part of "surveillance directed at a person reasonably believed to be overseas." This authorization could sweep in millions upon millions of private communications of Americans.

The PAA's exception to the definitions would seem to allow the government to acquire all communications by or from Americans to a group, corporation, or individual overseas, so long as such surveillance is directed at the group, corporation, or overseas individual. There is no limitation on who the overseas target is or how many overseas targets may be selected by the NSA's supercomputers. There is no requirement of any court supervision of such surveillance,

[1] It seems the administration believes that answering this question would reveal "sources and methods," but FISA's whole framework for protecting Americans' privacy is about having a public law setting forth clear limits on the "methods" of surveillance of Americans—what type of communications are protected, where, and how.

much less any requirement that if such surveillance acquires significant communications or a significant number of communications by Americans a warrant must be obtained. There is no requirement that anyone outside the NSA even be informed of how many communications by Americans are intercepted, analyzed or retained by the NSA's supercomputers.

The PAA's broad language also appears to authorize warrantless access to the domestic communications of Americans, so long as the government is not intentionally targeting a particular American and is seeking foreign intelligence information about a person abroad.

The plain language of the PAA goes even further than the international communications of Americans. Section 2 provides that if surveillance is directed at a "person" overseas (*i.e.*, is not "electronic surveillance,") the government can compel communications carriers to provide access to their US facilities if the government asserts, without any oversight, that the purpose is to acquire "foreign intelligence information concerning persons reasonably believed to be outside the US." There is no doubt that communications between two Americans in the U.S. could well contain foreign intelligence information concerning groups or corporations or governments overseas, which group, corporation or government may be the entity at which the government is directing its surveillance. Thus, the executive branch could authorize the interception or other acquisition of such domestic communications containing foreign intelligence, unless some other provision of the FISA prohibits such acquisition.[2]

While the administration carefully dodges these issues by referring to FISA's protections for domestic communications, the interplay between FISA and the PAA's new regime is such that the government could now acquire such domestic communications, so long as the government is not "intentionally targeting" "a particular known United States person who is in the United States." Thus, so long as the NSA is engaging in a broad, non-targeted surveillance program, it can acquire the domestic as well as the international communications of Americans in the US.

This is perhaps most easily seen by using a hypothetical example. The PAA can be read to authorize the acquisition of foreign intelligence information concerning the political leadership in India.[3] They can do so by directing the NSA to program its device for intercepting and analyzing communications at US facilities to select out and copy for the NSA all calls to or from a list of phone numbers belonging to the leaders of the major political parties in India, which would include all calls to or from Americans in the US, and the same for e-mail communications. Such acquisition appears to meet the requirements of subsection (a) of section 2 of the PAA.

But the administration could authorize much more. They could direct the NSA to program its interception and selection devices so that the NSA obtains all subsequent communications for some period of time by anyone who contacts or is contacted by any of the initial numbers or e-mails in India. Having thus acquired these communications, the NSA supercomputers can then search such communications for information concerning the Indian political parties, either by using search terms to scan the content or by determining whether such subsequent

---

[2] This point has been raised by former Justice Department official David Kris. *See* Slate.com.

[3] Such parties come within FISA's definition of "foreign power" and information about such parties can be said to relate to the conduct of the foreign affairs of the US as well as in all likelihood the security of the US and therefore constitutes foreign intelligence information under FISA.

communications were with individuals who might also communicate about those political parties. The only actual numbers or e-mail addresses plugged into the acquisition/selection device would be the original phone numbers or e-mails in India—the other directions simply consist of an algorithm directing the acquisition of the subsequent communications by individuals in contact with Indian leaders. Those subsequent communications could include contacts by Americans with other Americans.

We are very concerned that there may be nothing in FISA as amended by the PAA that would prohibit this and it seems clearly authorized by the legislation. It meets all the requirements: it is acquisition of foreign intelligence information about "persons" located outside the United States; it does not constitute "electronic surveillance" because it is surveillance directed at foreign political parties and it is not acquiring the content of any communication by a "particular known United States person who is in the United States" "by intentionally targeting that United States person." Quite to the contrary, not only are particular known Americans not being intentionally targeted, but when the surveillance begins, the NSA does not even know whether its algorithm will acquire any communications by any Americans. Thus, the essence of the PAA is to allow the NSA broad access to Americans' communications so long as it is done as part of an effort to collect foreign intelligence information concerning overseas persons, groups, corporations, or foreign political parties or governments.

Under the PAA's regime there is no independent check to monitor the deployment of computer sorting methods by NSA systems that may well be a permanent presence on the global telecommunications infrastructure in the US. There is no system for guarding the guardians exploiting new access to the global communications of Americans.

While we have seen repeated statements by administration officials attempting to dodge this issue, we have seen nothing categorically denying that the PAA would permit this. When confronted with this interpretation, the administration has not flatly denied it; their responses have been carefully drafted to the effect that they will continue to comply with the FISA's requirements for domestic surveillance. But those requirements have been changed, so that warrants are only required in much more narrow circumstances than before, such as the intentional targeting of a particular known US person.

The PAA paradox means that more collection results in less protection for more Americans.

The PAA changes seem to create a paradox that the less targeted the NSA is, the greater the number of communications it can obtain. The targeting language of FISA that was supposed to be a shield for privacy rights has been transformed into a sword. By not targeting particular Americans the NSA gains the power to obtain many more communications of Americans than ever before.

The PAA does not "restore" FISA authorization to monitor Americans here because there never was such authorization.

One of the administration's main assertions is that the PAA merely restores the "original intent" of FISA, by restricting the application of the warrant requirement. Their claim is that Congress

did not intend to require a warrant for international calls unless the government was "targeting" an American. This incorrect claim is followed by the false claim that back in 1978 all international communications came within the "radio exception" because they were carried by satellite (and thus accessible to NSA receivers) and all domestic communications were carried by "wire" (and thus inaccessible to NSA "ears") and that now the situation is reversed. These claims are wrong.

It is not correct to say that changes in technology have deprived the NSA of access to Americans' international communications that it was previously entitled to. To the contrary, FISA was intended to prohibit precisely the kind of NSA activity that now seems to be authorized by the PAA, the mass interception of international communications by Americans off the wires in the US.

The administration's description of the previous status quo is simply inaccurate as a matter of historical record. In 1978, it was already known that many and maybe most international communications of Americans traveled into and out of the country by wire, such as through the newer transatlantic cables that were laid in 1978.[4] And Congress specifically protected international communications traveling by cables in the US from interception without a warrant.[5] The legislative history specifically states that those international wire communications are covered by FISA if the acquisition of the contents of the communication occurs from the wire in the US, a requirement that was also explicit in the text of FISA, 50 U.S.C. 1801(f)(2). The use of transatlantic and transpacific cables to transmit Americans' communications was hardly unforeseen. Ten years after FISA was passed these metal cables were replaced by fiber optic ones. In the intervening twenty years the government did not claim a right to access Americans' communications on those cables without warrants, but now it does.

Moreover, FISA was enacted precisely to prevent NSA programs for the wholesale acquisition of Americans' international communications. FISA was enacted after the revelations about Operation Shamrock—an operation where the NSA had obtained copies of almost all international telegrams of Americans. The Congress and the NSA agreed that such programs should end and that agreement was reflected in FISA.

The administration's retroactive reading of FISA is inconsistent with that agreement. Its reading would have allowed the NSA to simply move Operation Shamrock to satellite interception. But the NSA at the time assured Congress that it rarely intercepted American communications. For example, in 1975 NSA Director Lew Allen promised Congress that the NSA was only targeting foreign communications channels, which carried only a minuscule number of international communications by Americans. *See* Letter from General Lew Allen to Chairman Pike, August

---

[4] It is also not true that purely domestic calls traveled only by wire—most long distance interstate calls were transmitted in part by radio towers. Because radio communications, now called "wireless" communications, between Americans could be accidentally intercepted through monitoring of the airwaves, Congress forbade "intentional" interception and was assured that communications accidentally or unintentionally intercepted would be "immediately destroyed."

[5] *See* S.Rep. No. 94-1035, 94th Cong., 2d Sess. 28 (1976); S.Rep.No. 94-1161, 94th Cong., 2d Sess. 26 (1976). Congress intentionally barred the tapping of wire communications without a warrant for "either a wholly domestic telephone call or an international call . . . if the acquisition of the content of the call takes place in this country . . . ." S. Rep. 95-604, at p. 3934 (1978).

25, 1975, confirming that the NSA was not "monitoring any telephone circuits terminating in the US." It was on the basis of such assurances that FISA's prescriptions for wiretapping were written.

In summary, the so-called radio exception was never meant to bless the deliberate, wholesale interception of channels carrying Americans' communications by the NSA without a warrant. FISA was based on agreement that the NSA was properly focused on foreigners overseas, not on Americans' communications. Amending FISA now to exempt from the warrant requirement any surveillance concerning a person or entity overseas and all their communications with Americans does not restore the status quo from 1978, it rolls back the clock to the era of Operation Shamrock. Such sweeping changes are a significant step towards adopting the viewpoint of those in the Justice Department and the White House that FISA and its procedures for judicial review unconstitutionally impinge on presidential power. The changes passed in August overturn the congressional/executive branch agreement of the past 30 years that giving the President such authority is unnecessary, unconstitutional and dangerous.

Changes in government surveillance technologies and increased contacts between Americans and the world require greater, not fewer privacy protections.

If allowed to stand, this law marks a fundamental change in the scope of surveillance operations of Americans' communications. For the first time, Congress will have authorized the NSA to turn its extraordinary technical surveillance capabilities, inward—to intercept Americans in the United States, rather than events overseas. The NSA, with its vast resources and technological capabilities, conducts surveillance on a massive scale and the PAA eliminates any requirement of targeted individualized surveillance based on a court's finding of probable cause. (While FISA did not bar the NSA's monitoring of international radio signals that might result in some incidental unintentional reception of Americans communications, the overall intent was to prevent the NSA from monitoring Americans or channels of communications of Americans.[6])

The administration has argued that changes in technology merit more power with fewer checks. While it is true that the intelligence community needs the capability to track down terrorists using modern communications technologies, there has been no demonstration that the most effective way to do this is to give the community carte blanche to surveil the communications of millions instead of requiring the kind of predicated and focused surveillance that would both protect Americans' privacy and make it more likely that intelligence efforts are focused on the right targets.

At the same time that vast increases in the power and range of surveillance technologies give the government greatly expanded powers to intercept and analyze communications, Americans are committing more and more of their private thoughts and communications to electronic form. And globalization has meant an exponential increase in international contacts by Americans—over 40 million Americans travel out of the country each year, for vacations, jobs, missionary work, health care or adoptions; almost half a million Americans serve in the military or work

---

[6] The radio exception "should not be viewed as congressional authorization of these activities" and Congress took pains to emphasize that "broadscale electronic surveillance" even of Americans who were abroad had been limited by the Executive. S. Rep. 95-604, at p. 3936 (1978).

overseas for the government; a couple million more live overseas; and about a quarter-million Americans study abroad every year. These Americans stay in closer contact with friends and family at home than ever before. In addition, more Americans work for or deal with foreign-owned companies than ever before in history, from J.C. Penney's to Dr. Pepper, and with outsourcing even contacts with American-owned companies can involve communication with foreign nationals. Americans routinely deal with many companies owned by foreign governments, which may come within FISA's definition of "foreign power." Plus, fully 80 percent of US ports are controlled by foreign-owned companies, including Chinese and Venezuelan companies.

This globalization calls for increased protections for the communications of Americans, wherever they may be communicating. Flexible judicial review is important for protecting Americans' privacy and freedom of speech and association by preventing the accumulation of massive databases storing Americans' private communications, even if those communications are not immediately disseminated.

After the fact "minimization" is insufficient to protect the constitutional interests at stake. As Senator Sam Ervin observed:

> [D]espite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy makes it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom.
> ...
> Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.[7]

The warrantless surveillance of previously protected American communications which appears to be authorized by the PAA epitomizes these dangers, given its reach into people's private lives without even any suspicion, much less probable cause that they are doing anything wrong.

The PAA eliminated other important protections.

In addition to the concerns addressed above, the PAA eliminates other key safeguards in FISA. It appears to:

---

[7] Senator Ervin,June 11, 1974, *reprinted in* COMMITTEE ON GOVERNMENT OPERATIONS, UNITED STATES SENATE AND THE COMMITTEE ON GOVERNMENT OPERATIONS, HOUSE OF REPRESENTATIVES, LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974 S.3418, at 157 (Public Law 93-579)(Sept. 1976)

- Allow warrantless secret searches of Americans' communications without even any after the fact meaningful oversight. As outlined above, the Act allows the interception and surveillance of Americans' domestic and international communications with no prior judicial authorization, no individualized determination of probable cause and no specification of which individuals or phone lines are to surveilled;
- Eliminate the requirement of fair notice to individuals that they have been overheard when they are indicted;
- Allow government access to stored communication records with no court orders or judicial oversight; and
- Allow the government to secretly obtain the call record information and other revealing meta-data on thousands or millions of Americans' communications with no judicial oversight, to conduct traffic analysis and construct maps of the associations and contacts of untold numbers of innocent Americans.

This recital may well be incomplete. As has been pointed out by others, there is no legislative record explaining either the understanding of the administration or the intent of Congress in enacting these amendments.

In addition to seeking to make these changes permanent (with only minor clarifications) the administration is seeking additional changes to the law. We strongly oppose these changes to FISA.

We believe there is no need to provide retroactive immunity to the carriers at this time or provide for substitution of the government. Doing so would eliminate a crucial check on government abuses. We oppose amnesty for companies as well as government actors, as called for by the administration's 2006 Statement of Administration Position on the Wilson bill.

In addition, we are very concerned that the administration may have already implemented by regulation, a proposal contained in its prior draft: namely that a warrant is only required for Americans' domestic communications if the government has reason to believe the sender and all recipients are in the US. That is, if the NSA does not know where you and all the recipients to your e-mails are at any given moment the government's position may be that no warrant is required. We have asked for the administration's assurances that they have not adopted such an unconstitutional presumption, but received none. The rhetoric of administration officials only underscores our deep concerns about the privacy of Americans' internet communications.

What is to be done?

As noted above, the PAA is unconstitutional and should not be made permanent. Neither Congress nor the American public has enough information yet to determine whether amendments are warranted nor what they should be. Without such information, it will be very difficult to draft changes that would prevent future violations of the law.

As outlined in the testimony of Dr. Morton Halperin before the House Judiciary Committee, the administration has not provided adequate information to show that amendments are needed. Their refusal to disclose information, varying public explanations, political posturing, and

selective disclosure of claimed classified information makes it impossible for the Congress to take them at their word, even if doing so were consistent with your constitutional responsibility.

We believe Congress should start by:

- Obtaining information about past surveillance activities in violation of the law;
- Ensuring adequate public disclosure about those activities; and
- Obtaining a binding public explanation of the administration's interpretation of each provision in the PAA.

This information alone is not enough. It is essential though because, as this committee knows well, the administration's rationale for why amendments to FISA are needed has shifted over time.

For example, while much of the administration's public rhetoric focused on the problem of having to obtain FISA warrants to intercept communications between two foreign terminals passing through switches in the United States, on occasion, they have admitted that such warrants have never been required by FISA. Moreover, the administration apparently also claims that the FISA requirement for warrants and court oversight should be eliminated because they cannot always tell where the parties to a communication are located. While this may be true some of the time or for brief periods, it is not true of the majority of Americans' communications. For example, many experts agree that it is relatively easy and quick to determine where the parties to any telephone call are located. The locations of parties to an e-mail may be more difficult to determine in some situations. But the administration has never offered a justification, nor do we believe there is one, for amending the FISA to eliminate the warrant requirement for all those international communications where it is reasonably likely that one end of the communication *is* located inside the U.S. And of course this problem provides no justification for allowing warrantless interception of domestic communications. Nevertheless, the PAA eliminated fundamental protections in FISA and appears to authorize the warrantless acquisition of many international and some domestic communications by persons *known* to be in the US, so long as the government's purpose is to collect information about a person believed to be overseas.

These and other potential issues cannot be adequately judged on the current record, because the administration has refused to disclose even a redacted version of the opinions by the FISA court and the legal arguments made by the government to the court. (We do not believe that the legal analysis – separate from identification of the surveillance targets – is properly classified. We have filed a Freedom of Information Act request for redacted versions of the courts' opinions and the legal arguments made by the government.)

Only after disclosure of all this information, can Congress consider whether permanent legislation is needed and what it should be. In addition, we believe the following general principles must be adhered to in considering any amendments to the FISA:

- The structure of FISA must be maintained;

- Surveillance must be carried out within the FISA structure—there should not be any change to the definition of electronic surveillance;
- Carriers must have the responsibility of sorting communications and insuring that the NSA is only given access to that which they are entitled to. Initial court authorization of surveillance in the US at US switches must be required;
- When the government intentionally acquires the communications of persons in the US, it must have a warrant to do so, which may authorize interception of the communications of either party to the call or e-mail;
- Acquisition of the increasing number of communications of US persons located overseas must comply with Fourth Amendment requirements;
- There may be limited exceptions for true emergencies, or when beginning surveillance of an individual target located overseas and it is not known whether the target will communicate with persons in the US; and
- Meaningful, mandatory and frequent reports to courts and Congress along with an IG audit must be required.

The draft bill crafted by Chairman Reyes and Chairman Rockefeller, described in the latter's August 1, 2007 news release appears to have incorporated many of these needed principles, but further public hearings on publicly available language would be essential to fully assess any such proposal.

Thank you again for considering our views.

The CHAIRMAN. Now, Mr. Rivkin, you are recognized for your opening statement.

STATEMENT OF DAVID RIVKIN

Mr. RIVKIN. I want to thank the Chairman and the Ranking Member and committee members who invited me to testify at what indeed is a very important hearing dealing with the legislation that is going to have some consequential and important impact.

A little bit about the past, since we can't understand where we are now unless we talk about the past.

Before the August recess, Congress passed a 6-month fix to FISA. I happen to believe, at least based upon everything I have read in the media—we know that the New York Times and other newspapers do have a pretty good access to what is going on in the government—that the fix was urgently needed because you indeed had a serious truncation of a collection stream largely as a result of the fact that FISA, which was heretofore a warrantless surveillance program that we talked about a little bit earlier, was put under the FISA jurisdiction in January of this year and within a few months there were some orders by the FISA court that impaired important intelligence collection efforts.

In response to these developments, Congress amended FISA specifically to permit surveillance of international communications of overseas targets without a court order, even if that interception occurs within the United States.

Now we heard a number of my colleagues who are concerned about privacy—so am I, for that matter—who fear that this approach may entail the interception of communications by American citizens; and indeed that has emerged as the pivotal question in the FISA—long-term FISA operation.

Again, a little bit about the past. I happen to think, in all candor, that today's fears stem from a certain ignorance about the past. I happen to believe, with all due respect to Mr. Baker, having looked carefully at FISA history that the notion—and let us leave little things like the Shamrock program aside—but the notion that I think a lot of privacy advocates would have you believe, that Congress enacted FISA to provide a comprehensive regulation of all or nearly all surveillance activities, is just plain false.

If you look at the statute itself, it outlines four fairly narrow scenarios.

The Congress in 1978 chose to deal with a discrete portion, in my opinion—and the facts do show that—of government's intelligence gathering. It really was focused on surveillance inside the United States. And, by the way, there is nothing particularly sacred about the distinctions made between wire and radio/satellite. Both distinctions were meant as a proxy to basically effectuate congressional desire to deal with surveillance inside the United States conducted in large part to get at Americans. And, let us be honest, there were some abuses in this area and not just by the Nixon administration but some of his predecessors, and that is what Congress primarily wanted to get at.

So FISA generally required the executive branch to obtain judicial orders where the actual surveillance target was physically present in the United States. For targets located overseas, court or-

ders were not required before a President could authorize an overseas wiretap with regard to radio communications, were not required whether or not the intercept was here or in the United States.

Now Congress knew that NSA was vacuum cleaning and indeed, not in any pejorative sense, as large of a data stream of foreign communications using its satellites and listening posts overseas. Did not bother anybody.

Incidentally, apropos of all the points about American-generated data, voice information, whatnot, getting commingled in that stream, I wouldn't deny it. But it has always been the case. I would kind of ask my colleagues rhetorically, what do you think happened in 1980 if we were targeting using the satellites, communications of somebody within Russia or China and that person called the United States 20 times? The communications, the American portion of the communication was not listened to? Did it require a warrant? No, it did not. Not at all.

We all heard about the revolution of communications and the fiber optic systems today. It is indeed true that more of the truly global traffic foreign-to-foreign flows from American fiber optic networks. So we do have circumstances today with an individual in Pakistan calling someone in Afghanistan has that communication routed from American fiber optic systems.

Incidentally, the parties to that call do not know how their call will be routed and are not in the best position, as I understand it—I am not an engineer—but not in the best position to determine what the path would be. Unlike my colleagues here, instead of being horrified by that, I think it is great. It gives NSA wonderful opportunities to tap into the global communications traffic that ought to be exploited.

Now let me quickly get to the heart of this matter.

What is the privacy concern about Americans? The concern is what I would call an innocent bystander scenario. We have a bad guy overseas calling somebody in the United States. This person is not an agent of al-Qa'ida, not a sympathizer. He is just an innocent bystander. I would stipulate that it happens. What puzzles me is that nobody seems to acknowledge that that scenario is not an unacceptable consequence of any particular FISA regime but it is endemic to all surveillance.

Warrants result from a process—and my colleagues love warrants—but warrants result from a process that considers the rights of a particular target or targets, not those who come into contact with them.

Let me tell you something. Under a Title 3 situation, which is the basic wiretap statute, when you get a warrant against a given criminal, be it a member of a Colombian mafia or an Italian mafia or just a downright criminal, that person comes into contact daily with dozens of innocent people. Could be his son's teacher, could be his grocer, his tailor. All of those people get caught in a wireless surveillance net, and nobody seems to mind that.

But the fact that the original decision to target that person is driven by a Title 3 warrant does absolutely nothing to protect the privacy of those other innocent Americans who, in a lexicon of my colleagues, are being spied at. I would rather be spied at in that

way in the context of a FISA-driven program because of the minimization requirement. To the best of my knowledge, there are no minimization procedures in the criminal justice system.

So this situation is not new. It is not novel. It was the case before, and it is the case today every day. Nobody has invented a way of discerning that a target of surveillance culls an innocent person and turning off the tap. That does not exist.

We heard a lot about law. We heard about the fourth amendment. If one reads the fourth amendment, the very language of the fourth amendment suggests that there can be "surveillance or searchings"—is the language they use—to provide warrants. Otherwise, it makes no sense. Because, in the front part, they talk about unreasonable searches being banned; and, in the second part, it talks about what is the basic process, what are the predicates of a basic warrant. So the fourth amendment only prohibits only unreasonable searches and seizures.

A lot of people claim that warrantless searches are inherently unreasonable, but that ain't so. That is not what the Constitution says. That is not what the case law says. And the Supreme Court over years has approved numerous warrantless searches. There is a whole line of cases called the "special need" cases. When you get stopped driving on Christmas in a sobriety checkpoint, there is no warrant, there is no particular suspicion. In fact, apropos of the business about targeting, the cop who stops you doesn't know who you are, does not know if you are a woman or man or Member of Congress. Has no idea.

When people search lockers in—students' lockers in high schools, they don't have any particularized suspicion that there is some contraband in there. And Customs agents searched you long before September 11th when you crossed the broader thinking that maybe you didn't declare everything that you bought in Paris. There are no warrants.

Believe me, all of those cases, all of those procedures have been challenged; and all have been upheld. And, as a matter of fact, unlike the kind of surveillance we are talking about, the fruits of those searches actually get used in criminal prosecutions.

I would challenge anybody who is stopped at a warrantless sobriety check and found to be legally drunk, I would challenge this person to successfully suppress this information in any prosecution for DWI. It is not going to work.

I am tired of hearing this notion that the Constitution requires a warrant in all circumstances.

Now the Constitution also requires reasonable expectation that privacy be protected, not all expectation of privacy. Again, there are lots of cases dealing with instances where somebody is growing a marijuana plant in fairly plain sight on a windowsill behind a picket fence and a police officer walking by, sees it. Well, gee, there is no warrant. No, if you are doing something in plain sight, if you are not acting in a way that gives rise to a reasonable expectation of privacy, it doesn't work.

I certainly don't understand why any intelligent reader of newspapers—you heard about things like Echelon, which I am sure you know what it is, but for those who don't it is a cooperative intelligence program that involves half a dozen of our allies that engage

in mobile surveillance. And there are dozens and dozens of intelligence services in charming places like Pakistan and Saudi Arabia. So if somebody calls Peshawar and that person does not understand that half a dozen of intelligence services on that side of the ocean are going to listen to him or her, that person does not have reasonable expectation for privacy; And the law and the Constitution does not require us to humor unreasonable expectations of privacy.

And as to foreigners, again, forgive me, the notion that if the bad guys knew there were two compartments, two regimes, if you did purely foreign-to-foreign communication, if you called somebody from Pakistan to Afghanistan, you were enrolled in the warrantless surveillance, but if you called enough times the United States, you had, you know, whatever is the balancing test here. If you brought enough Americans into your circle, you would graduate into a warrant-driven program. Any bad guy, unless he is an idiot, would call. Every spymaster in the world, every terrorist would call the United States enough times to order pizza or something from Borders.

So everybody would be in a warrant-driven surveillance program in a situation where none of those people have any reasonable expectation of privacy

Now, look, I think we should be honest. Extending the warrant's requirement—against whom are we going to get warrants here? We are not going to get warrants against innocent American bystanders. You couldn't. There would be no predicate for getting warrants. Just because you get a call from a bad guy does not make you subject to a warrant. We are talking about getting warrants against foreigners.

I happen to think the FISA court is not a rubber stamp. Nor should it be a rubber stamp. Because what would be the value of getting it?

So we are going to get warrants against—we are going to have NSA get warrants against foreigners after they—whatever is the threshold—called the United States enough. We frequently don't know who they are. We don't know their age. We don't know their real name. We may have a secondary or tertiary idea that the individual involved may be a cousin of somebody who knows an al-Qa'ida person. You are not going to get a warrant against such a person. I would be ashamed to ask a FISA court for a warrant against that person because there would be no basis for it.

So, basically, what we are going to see is a serious truncation, a serious decrease in the number of foreign targets that could be serviced.

Let us be honest. What would that do? It would not be great for our national security. Let us be honest. It would definitely diminish the number of innocent Americans whose conversations would be heard. That is actually the trade-off that some of my privacy focused colleagues are suggesting.

The best way of making sure that fewer Americans get their communications, minimization and everything incidentally intercepted, is there are pure foreigners whom we are going to service as targets. Because that is really the reason. If the number of foreigners in that warrantless program is a million and the number of foreigners in a warrant-driven program is a million, you still are

going to have exactly the same number of Americans whom they are going to contact and the same quantity of American information.

In order to protect a very incidental impact, in my opinion, and privacy—and again I don't have time—but, to me, my privacy is violated when something bad happens to me, when I am confronted with something. Just because somebody heard my conversation or may have heard my conversation doesn't bother me particularly, and I suspect that is true of most Americans.

At the end of the day, privacy has to be balanced against other societal goals and expectations, and the very least I would urge you to do is to look at how Americans balance privacy in other spheres. Credit card companies know more about us than the NSA does.

Every time we have an episode like the Virginia Tech shooting that are regrettable, there are proposals being floated for dissemination of truly private medical information without judicial involvement where you share this with school administrators and whatnot. And not to minimize what happened at Virginia Tech, but I would submit to you that the threat we face from al-Qa'ida is somewhat higher in terms of its consequences of this country than the threat of a deranged gunman.

So we, as a society, can balance liberty/privacy and public safety. But let us be consistent. Let us not adopt the position that we should balance it one way in the context of external threats involving al-Qa'ida, where we push the pendulum towards the privacy side way beyond what it was in 1978. But then it comes to other issues like Virginia Tech or drunk driving or something like that, you know, we will do it differently because that is a fundamental sign of dysfunction and rationality.

I look forward to the questions.

Thank you.

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

[The statement of Mr. Rivkin follows:]

Statement of David B. Rivkin, Jr.

Partner, Baker Hostetler LLP
Former Department of Justice and Office of the White House Counsel Official

Before the

House Permanent Select Committee on Intelligence

Foreign Intelligence Surveillance Act and NSA Activities

Tuesday, September 18, 2007

I would like to thank Chairman Reyes, Ranking Member Hoekstra, and other Committee Members for inviting me to testify at this hearing on the Foreign Intelligence Surveillance Act ("FISA") and the authorities for the National Security Agency's ("NSA") surveillance activities.

Before the August recess, Congress passed a six-month "fix" to FISA. FISA generally requires a judicial order before the Government can intercept "electronic communications" in the United States for foreign intelligence purposes. The fix was urgently needed because the "warrantless" component of the NSA's post-September 11 "terrorist surveillance program" – directed at al Qaeda global communications and brought under FISA earlier this year – had been dramatically narrowed by the special FISA court in a decision that impaired necessary intelligence collection efforts.

In response, Congress amended the law specifically to permit surveillance of international communications of overseas targets without a court order, even if the interception itself occurs in the United States. Unfortunately, vocal privacy advocates oppose this approach, largely because it may entail the incidental interception of communications by American citizens who, while not terrorist themselves, may nevertheless be in contact with al Qaeda operatives. The emotional issue of privacy seems likely to dominate the unfolding FISA debate. Unless properly addressed, the privacy concerns threaten to derail efforts to enact a permanent reformed FISA. Such an outcome would drastically reduce America's intelligence intake and

increase the risk that Jihadist forces may succeed in once again attacking the United States or our allies.

At one level, today's privacy concerns are rooted in lamentable ignorance about the past. Congress' recent action to exclude foreign communications where the target of the surveillance is overseas from FISA's "warrant" requirements simply returned the law to its original intent. When FISA was enacted in 1978, it did not regulate all, or even most, of the federal government's surveillance activities. Rather, Congress opted to deal with only a discrete portion of the government's intelligence gathering, focusing only on surveillance inside the United States or otherwise targeted at Americans. It made this choice largely because the Nixon Administration (and its predecessors) had justified a wide spectrum of domestic wiretapping on the basis of foreign intelligence needs. The U.S. targets of these activities often suffered real consequences, ranging from criminal prosecutions to other adverse governmental actions.

At the time of FISA's enactment, even the strongest congressional proponents of the statutory regulation of surveillance activities recognized that intelligence gathering was a key executive function and that the U.S. needed to collect as much foreign intelligence as possible. This bi-partisan consensus that FISA compliance could not be allowed to impede foreign intelligence collection was all the more notable, as it arose during a period of congressional activism directed at regulating Executive Branch activities and at a time when Cold War threats, while formidable, did not require a constant real time surveillance of a diverse array of non-state groups.

Consequently, the new law required the Executive Branch to obtain judicial orders where the actual surveillance target was physically present in the United States. For targets located overseas, court orders were not required before the President could authorize an overseas wiretap, or an intercept of their radio communications, whether collected overseas or in the United States. At the time, of course, most of this foreign intelligence collection was

accomplished by NSA satellites and "listening posts" located outside of the United States. These allowed NSA to intercept vast quantities of global communications without any warrants or, indeed, any kind of judicial involvement.

Today, primarily because of the revolution in communications technologies, the United States' excellent communications networks attract a large percentage of the world's message traffic. As a result, the same kinds of communications between non-U.S. persons overseas that were once intercepted overseas, now flow along fiber optic networks physically located in the United States. They nevertheless remain foreign communications between non-U.S. persons. These communications are thus properly subject to warrantless interception under FISA. By permitting the interception of these communications without a FISA court order, Congress has simply restored the original balance struck in 1978.

This history aside, the privacy-related arguments made by the Administration's critics are both vastly overblown and simplistic. They usually assume that the privacy interests of Americans and foreigners are equally worthy of protection, that all privacy impairments are equivalent, and that the mere possibility that somebody's conversation may be overheard without a warrant *per se* constitutes an unacceptable invasion of privacy. Even more problematic is the critics' manifest failure to emplace the FISA debate into the broader context of the ongoing debate in American society about how to balance privacy and public safety. For most Americans, indeed, privacy interests do not trump all other policy imperatives. The end result is an intellectually sterile discourse that does an injustice to all of the nuances and complexities of the privacy issue in modern America.

To begin with, despite all of the emotion surrounding the "innocent American bystander" scenario, far from being a unique and unacceptable consequence of a particular FISA regime, it is endemic to all surveillance. Warrants and other judicial surveillance orders result from a process that considers the particular target's rights. They are not designed particularly to protect the myriad of others who may come into contact with the target and, in the process, also

may have their communications intercepted. At least under FISA, and unlike the case with criminal justice-related surveillance, the Government follows "minimization" procedures – governing how the information is handled to prevent its inappropriate use, dissemination or disclosure – that protect the innocent bystander's privacy. The fact that senior U.S. government officials, unlike their counterparts in other countries, do not get access to the unredacted surveillance-generated information about American citizens and that the system is operated largely by career civil servants, provides additional layers of privacy protection.

Significantly, as explained by CIA Director Michael Hayden in 2006, elaborate minimization procedures are also employed as a matter of practice when foreign intelligence was intercepted, outside of FISA's framework, overseas: "if the U.S. person information isn't relevant [without foreign intelligence value], the data is suppressed." Indeed, it is precisely because warrantless surveillance is conducted in secrecy, with the utmost care being taken that the individuals involved never learn about it, that it is arguably the most privacy-protective. Meanwhile, the number of innocent bystanders, whose privacy has been impacted, will not be diminished if NSA has to seek warrants for all or most of its overseas targets. In either case, an innocent bystander would never know whether a warrant had been issued and hence, could not structure his conduct to minimize the chances of being caught up in the surveillance net.

Making all NSA surveillance warrant-driven is also not required as a matter of law. The Constitution's Fourth Amendment prohibits only unreasonable searches and seizures. Although today's privacy advocates routinely claim that a warrantless search is inherently unreasonable, this position is not supported by the Constitution or the case law. Over the years, the Supreme Court has approved numerous warrantless searches, balancing the government's interests against the relevant privacy expectations. Thus, drivers are subject to sobriety checkpoints and international travelers to search at the border because their reasonable privacy expectations in these situations are limited. Moreover, unlike the case with warrantless NSA surveillance, the fruits of these other warrantless searches are routinely used in civil and criminal prosecutions.

It is difficult to see why foreign nationals communicating abroad have any reasonable expectation of privacy vis-à-vis the United States Government simply because their conversations may be electronically transmitted through American switching stations. Similarly, when Americans make or receive international calls that may be incidentally intercepted because of overseas surveillance, they have a reduced expectation of privacy. Dozens of foreign intelligence services, some belonging to global powers such as Russia and China who have counter-terrorism concerns of their own and others working for regional powers, routinely intercept as many international communications as they can. The odds of interception by some intelligence service grows exponentially whenever an American communicates with people in countries, such as Pakistan, Iraq, Afghanistan, where significant terror-planning activities are known to occur. Meanwhile, some multinational companies also engage in industrial espionage, intercepting in the process at least some global communications. In short, the notion that privacy exists in today's globalized world is largely a myth.

The knowledge of these facts is readily available to even a casual newspaper reader, enabling Americans to structure their overseas communications in ways that satisfy the extent and intensity of their privacy concerns. Far from being uniform, privacy concerns vary among Americans. Even for the same person, their intensity depends upon many factors, including who intercepts their communications, whether they are confronted with this fact, and what other foreseeable consequences, if any, could ensue as a result of the intercept. Many Americans do not care much about solitude and routinely tell the pollsters that they are untroubled by the fact that the government may listen in on their calls. Others are more guarded in their expectations, and some treasure their privacy above all else.

In possession of all the facts about the all-too porous nature of overseas communications, an American who seeks to ensure that his private dealings remain private from all comers and who wants to talk to a person in a Pakistani village, would be well-advised to do so in person. By contrast, a less privacy-phobic innocent American bystander may be quite

happy telephoning Pakistan, either because he never knows for sure that his side of a conversation with an overseas target is being listened to, or at most, suspects that this might be the case, or just plain does not care. More fundamentally, irrespective of his precise privacy-related inclinations, because no adverse consequences will ensue if even a half-dozen intelligence services listen in, his privacy is compromised in a comparatively attenuated fashion.

However, expanding FISA's "warrant" requirements to the collection of all or virtually all foreign intelligence is certain to cripple the United States' intelligence gathering capacity. This would create a particularly acute problem in a protracted war against a shadowy and committed enemy, in which defectors are rare, the CIA's chances of penetrating al Qaeda's inner councils are slim to none, and aggressive interrogations of captured Jihadists have become increasingly unpopular. The widest and most proactive surveillance operations, targeted on every segment of the far-flung Jihadi network, have become the most vital aspects of U.S. intelligence gathering. They have proven their worth in stopping numerous terrorist attacks, with the German plot being the most recent example.

The United States' ability to continue with this strategy will be undermined if privacy protection becomes the overarching imperative of U.S. intelligence policy. Because the special FISA court is not a rubberstamp, it would be impossible to obtain orders against many foreign targets about which comparatively little may be known, including their true identities or the precise modalities of their involvement with Jihadist entities. And, of course, if the FISA court became a rubberstamp, obtaining its orders would not enhance privacy protection.

Those who want to subject all government surveillance activities to a warrant requirement should honestly acknowledge that this approach would dramatically shrink the stream of foreign intelligence. They must be prepared to justify their approach on that basis. Moreover, instead of waving the privacy banner in an undifferentiated fashion, the critics should explain what privacy interests of innocent American bystanders are actually threatened by a warrantless surveillance regime, in what way they are actually compromised, and how the

degree of hardship imposed compares with other privacy compromises that Americans have accepted in the recent past.

Unfortunately, the current debate over privacy and FISA reform has been both simplistic and dominated by political correctness. Thus, for example, none other than the Chairman and Vice Chairman of the 9/11 Commission, writing on the sixth anniversary of the 9/11 attacks, proclaimed that "we're not safe enough," yet lamented warrantless surveillance practices. It is possible to worry about the continuing shortfall in U.S. intelligence gathering and want it augmented; it is also possible to condemn all warrantless surveillance as a threat to U.S. civil liberties and want it banned. Holding both of these views simultaneously, however, is hard to justify.

Moreover, unlike many other war on terror-related policies, such as the handling of enemy combatants, which represent significant departures from peacetime norms of balancing liberty and order which have become deeply ingrained in American legal and political cultures, the FISA debate should be an easy one. Individual privacy is, of course, an important interest. It is not, however, the only important interest. Privacy must be balanced against society's legitimate need for security, whether arising in the war on terror context or in the context of protecting college students from harm caused by deranged shooters. Indeed, a rational society would certainly want to balance privacy and public safety in a consistent manner, across the entire range of threat scenarios. In this regard, it is significant that even domestic public safety problems, such as the recent and tragic shootings at Virginia Tech, routinely lead to proposals to liberalize the sharing of sensitive private information and do so without court involvement.

Restoring FISA to its 1978 scope, which did not prevent NSA from obtaining warrantlessly as much intelligence about overseas targets as possible, strikes an appropriate balance between privacy and safety. In a post-September 11 world, American society cannot afford to elevate privacy concerns beyond all other considerations. The notion that the balance struck between privacy and security in 1978 is somehow inherently inappropriate today and

needs to be recast with security taking the back seat is hard to credit, especially since the need to obtain more intelligence information, and to connect the dots, was one of the 9/11 Commission's most important conclusions.

To the extent that Congress is concerned with potential abuses and wants to bolster the political accountability of the program, it should require enhanced minimization procedures and additional intelligence oversight – perhaps by expanding the current "gang of eight" congressional leaders, who are regularly briefed on intelligence operations. It may also be worthwhile to have Congress review the entire range of possible consequences for an innocent American bystander whose conversations with an overseas target have been intercepted; so as to ensure that such people do not automatically find themselves, for example, on a no-fly list.

Expanding the reach of the FISA court, and limiting in the process the United States' ability to acquire foreign intelligence vital to the security of all Americans, is the wrong way to proceed. Instead, Congress should act to make the recent FISA fix permanent by enacting the Administration's sorely-needed FISA Modernization proposals. At the very least, Congress should make permanent the Protect America Act of 2007 and should immunize from lawsuits those business entities which cooperated with the Administration during the earlier phases of the NSA surveillance program.

The CHAIRMAN. In consultation with the ranking member and pursuant to Rule 11–2(j) of the House rules and Rule (d) of the Intelligence Committee's Rules of Procedure, there will be 30 minutes divided equally between the majority and minority staff of questioning of the witness. Following staff questioning, the committee will proceed with witness questioning by members under the 5-minute rule, exclusive of the ranking member and the chairman.

So I now yield 15 minutes under this section to Jeremy Bash, Chief Counsel of the committee.

Mr. Bash, you are recognized.

Mr. BASH. Mr. Baker, you started at the FISA office in 1996, and you were the seventh attorney supporting intelligence operations there, is that right?

Mr. BAKER. That is correct.

Mr. BASH. And you ran the FISA office as counsel for intelligence policy for nearly 7 years during the Bush administration.

Mr. BAKER. Clinton and Bush administrations, that is correct.

Mr. BASH. Did FISA provide the government with timely, actionable intelligence on terrorist targets after 9/11 during wartime?

Mr. BAKER. Yes. As I suggested in my oral statement today, we obtained quite a bit of actionable foreign intelligence, which to me means timely, pursuant to the FISA process.

Mr. BASH. The FISA office is sometimes characterized or caricatured as creaky, outdated, not keeping pace with technology. What is your response to that?

Mr. BAKER. We have also been called a rusty gate, other things like that, too.

I don't think that was accurate, those types of characterizations. As I said in my oral remarks, we were able to construct a process that I think at the end of the day provided the Intelligence Community with a lot of actionable intelligence.

At the same time, you can always do more if you have more resources. And so I think if you go back and look at the history of OIPR, we have grown over time, especially since 1996 until I got there, certainly until today; and the more folks you have, the more you can do.

Mr. BASH. Some have suggested that the FISA operation is very slow to approve surveillance in "no kidding" emergencies. Under FISA, the Attorney General can authorize emergency approvals. Can you walk us through how fast that can happen?

Mr. BAKER. Well, I think I have testified in this committee in closed session before about the process. We try to make it as quick as we possibly can. There are a number of different things going on. But let me back up.

So the Attorney General can authorize—and Attorney General here means the Attorney General, the Acting Attorney General, the Deputy Attorney General or the Assistant Attorney General for national security. So any one of those folks can authorize an emergency FISA.

The way it works is—I am sorry—and it goes for 72 hours, and if you want to use that material or continue the surveillance or the search, you have to go to the FISA court within that—or by that time.

So we work with the Intelligence Community to understand their needs and prioritize their requests. So often what will happen is we will work on dual tracks. So the Intelligence Community will notify us, hey, there is an emergency that we are working—we can see already that we want to do an emergency surveillance, let us say. We are working, in particular, let us say, the FBI. We, the FBI, are working to put our ducks in a row from a technical basis to implement the surveillance because it takes a little time. And while they are working on technical stuff, we are working on the legal stuff. The idea is that the trains cross the finish line at the same time, and when they are ready to go, we are ready to go, and we call the Attorney General, and that is it.

Mr. BASH. How fast can it happen in an emergency?

Mr. BAKER. It can happen extremely quickly. We have done it in a very short time, minutes sometimes. That is when you have everything ready, everybody has been working together, and they are not ready to go with the collection until they tell us. It is done in hours. It is done in the same day. It is done as fast as they tell us they need it.

Mr. BASH. Directing your attention to the administration's bill, which has been called the PAA, is there anything in the PAA that streamlines the FISA process or the traditional FISA process, anything that would accelerate the approval of FISAs in emergencies?

Mr. BAKER. I don't think that it—well, in terms of a traditional FISA emergency—I mean, there are emergency provisions built within the PAA for the PAA type of collection. For traditional emergencies, I don't see anything in there to do that, no.

Mr. BASH. In a letter to the chairman last week, September 14th, Assistant Attorney General Ken Wainstein, wrote that the language of the PAA does not authorize physical searches of the homes or effects of Americans without a court order. Do you agree with that reading of the statute?

Mr. BAKER. Physical searches of the homes or effects of?

Mr. BASH. Americans without a warrant.

Mr. BAKER. Well, under the PAA, it is a somewhat complicated analysis to get to that question.

Let me say first that—and I am aware that there has been a letter. I haven't had time to study it, quite frankly. What I would say is a letter from the Assistant Attorney General for national security for the Department, while not an opinion from OLC or an opinion from the Attorney General himself, it is obviously within the executive branch, going to carry a lot of weight. So it would seem to me that it would be—were the administration to change its view on that, it would have to explain that, I guess, to the FISA court or——

Mr. BASH. In your reading of the statute, do you believe the statute, the plain meaning of the statute, could be read to authorize physical searches inside the United States without a warrant?

Mr. BAKER. It is a complicated analysis; and if you want me to walk through it, I can.

I think the short answer is that if you take an aggressive reading of the statute and you presume that you are going to be directing your surveillance at persons overseas and yet somehow looking for their communications in the United States on communication

equipment or related equipment and you can somehow work your way through the statute to obtain the assistance of a communication service provider or other person but you have got to go through all of these different steps, you can construct an argument that the statute allows something like that.

But again, as I understand it, Mr. Wainstein has said that the executive branch is not going to interpret it that way, and that I think is binding on the executive branch right now.

Mr. BASH. Have you been in a situation or a crisis where there is a strong push in the executive branch to push the law to its logical limits?

Mr. BAKER. Over the years, I have been in situations—many years—where aggressive and well-meaning attorneys throughout the government push aggressive interpretations of the law.

Mr. BASH. And have you argued matters in the FISA court?

Mr. BAKER. Many times.

Mr. BASH. In interpreting FISA, would they look first at the plain meaning of the statute or would it first look at a letter from Ken Wainstein for guidance on what the statute means?

Mr. BAKER. Well, I guess if Mr. Wainstein is on record already, it is going to look at that in terms of his interpretation.

Mr. BASH. Does his letter have the force of law in the eyes of the court?

Mr. BAKER. In the eyes of the court, no. It is not an act of Congress. It is not a judicial decision. As I say, it has a binding effect on the law as it is implemented or enforced by the executive branch.

Mr. BASH. You were counsel for intelligence policy on 9/11?

Mr. BAKER. That is correct. I was acting counsel.

Mr. BASH. And when the White House decided to establish a surveillance program outside of FISA, you were not consulted; is that right?

Mr. BAKER. We are talking about the terrorist surveillance program? Well, the terrorist surveillance program was already—it was already in existence when I was informed of it.

Mr. BASH. So you were informed of it after it was already in existence.

Mr. BAKER. That is correct.

Mr. BASH. So when it started, you were not briefed into it?

Mr. BAKER. Well, it was our—I guess the only thing I can say in a hearing today, I was not aware of it. It was already in existence when I became aware of it.

Mr. BASH. Do you think that those who established the NSA's surveillance program on the grounds that FISA may not have been agile or fast enough might have benefited from the perspective of the person who had been running FISA operations within the government?

Mr. BAKER. Well, I obviously had a lot of experience with FISA and knew what we were capable of at the time, I guess is the only way I can answer that question.

Mr. BASH. Your former colleague, Jack Goldsmith, head of the Office of Counsel Legal, writes in a forthcoming book that Vice President Cheney's Chief of Staff said, quote, we are one bomb

away from getting rid of that obnoxious FISA court. Is that quote accurate?

Mr. BAKER. I don't believe that today I can—that I am in a position to confirm or deny exact quotes about what people said.

Mr. BASH. Do you have knowledge of the accuracy of that quote, but you cannot confirm or deny? Do you have knowledge of the accuracy of that quote?

Mr. BAKER. I have knowledge of the accuracy of that quote, I guess.

Mr. BASH. Goldsmith also says that the people in the administration treated the FISA the same way they handled the other laws: Quote, "They blew through them in secret based on flimsy legal opinions that they guarded closely so that no one would question the legal basis for the questions."

Were you one of those questions whom they guarded those flimsy legal opinions from at the outset of the program?

Mr. BAKER. Well, as I said, the program was already in existence when I found out about it. Over time, over time I had access to legal opinions with respect to the program.

Mr. BASH. Those would be the Office of Legal Counsel opinions?

Mr. BAKER. Well, I think I would like to say I had access to legal opinions with respect to the program.

Mr. BASH. If committee members wanted to understand the administration's rationale for the program, would it be beneficial for the committee members to review those legal opinions?

Mr. BAKER. Well, I mean, I am obviously in a difficult position here. I think the answer is that in order to understand what happened, it is helpful to understand the legal thinking behind it.

Mr. BASH. Do you know if they had been provided to the Congress?

Mr. BAKER. My understanding is from the Chairman's remarks earlier that they had not been provided.

Mr. BASH. Mr. Dempsey, in an interview in the El Paso Times, August 22, 2007, the DNI explained the three provisions that he sought in the legislation. He said, "I was after three points: first point, no warrant for foreign or overseas." Let me stop there.

Do both the Democratic leadership bill, H.R. 3356, and the administration bill eliminate the requirement for individual court orders for foreign targets overseas?

Mr. DEMPSEY. Yes, they both did that.

Mr. BASH. Second, the DNI says "liability protection for the private sector," and by that I think he clearly meant lawful compulsion of the private sector. Do both the Democratic leadership bill, H.R. 3356, and the administration bill provide for lawful compulsion?

Mr. DEMPSEY. The PAA doesn't address the issue at all. The administration has pushed the bill that would provide both prospective immunity, which is in 3356, and the administration bill would also retroactively forgive the companies, give them immunity for their violation of FISA.

Mr. BASH. But the PAA and the Democratic leadership both address the issue of compulsion?

Mr. DEMPSEY. They both address—well, PAA does it through an Attorney General order. The H.R. 3356 does it through a court order.

Mr. BASH. In your view, is a court order a better mechanism for compulsion?

Mr. DEMPSEY. I think it gives the companies greater certainty. One of the purposes of the exercise here is to provide clarity and certainty.

Mr. BASH. Further, the DNI says there must be a requirement to have a warrant for surveillance against the U.S. person. Do both the Democratic leadership bill and the administration bill, provide for obtaining the warrant requirement for surveillance against U.S. persons?

Mr. DEMPSEY. Well, the whole question turns on what you mean by "against a U.S. person." The administration bill, the PAA, has a very narrow definition of what is surveillance against an American person. The 3356 bill has, I believe, a more balanced and appropriate view of when an individualized warrant should be required, and it has a mechanism for ensuring that those orders are sought appropriately.

Mr. BASH. On balance, given those three criteria that the DNI laid out, which bill, the PAA or the Democratic leadership bill, did a better job at accomplishing those three objectives?

Mr. DEMPSEY. I think by far the more balanced bill is what you referred to as the Democratic bill, H.R. 3356.

Mr. BASH. Ms. Graves, let me just close with you. Under the PAA, can the executive branch monitor, without a warrant, telephone calls between an American citizen in, say, Florida, talking to his sister in Spain?

Ms. GRAVES. Definitely.

Mr. BASH. Can the executive branch read, without a warrant, the e-mails of a doctor in Chicago with his colleague in Toronto?

Ms. GRAVES. Yes.

Mr. BASH. Let me push the hypothetical a bit. Would the PAA authorize the government to monitor, without a warrant, all the communications between a city, say, in New York and another country, say, England without a warrant?

Ms. GRAVES. All the communications between the U.S. and any other country.

Mr. BASH. Could the PAA authorize physical searches of Americans' homes?

Ms. GRAVES. It certainly is ambiguous with respect to the term "acquisition," and we do not believe that ambiguity should be allowed to stand.

Mr. BASH. What about with respect to offices and computer hard drives?

Ms. GRAVES. It certainly seems to reach that.

Mr. BASH. Medical records, library records or financial records, would the PAA authorize warrantless collection of those?

Ms. GRAVES. Without limitation, they are not specified or carved out.

Mr. BASH. In all those hypotheticals, who would make the determination as to who would be appropriate targets for surveillance?

Ms. GRAVES. Solely the executive branch, the Attorney General and the Director of National Intelligence.

Mr. BASH. Would that determination be reviewed by a court?

Ms. GRAVES. No.

Mr. BASH. Would that determination be reviewed by Congress?

Ms. GRAVES. No.

Mr. BASH. The final question is, would that surveillance ever be reported to Congress?

Ms. GRAVES. No, certainly not, if past history is any indication of the level of cooperation or information.

The CHAIRMAN. Thank you, Mr. Bash.

For the members, we have three votes that have been called. There is about 7 minutes left. The Journal is the first vote; the previous question on the FHA bill is the second vote. That is a 5-minute vote. And then the rule on H.R. 1852, the Expanding American Homeownership Act. That is also a 5-minute vote.

I am going to recess the hearing for members to go vote, then welcome back and recognize Mr. Donesa. When we come back, we will recognize the minority side for their 15 minutes. With that, we recess the hearing for about 20 minutes.

[Recess.]

The CHAIRMAN. The committee will please come to order. The Ranking Member has requested that he be allowed to control the 15 minutes of minority staff time.

With that, I now yield 15 minutes to the Ranking Member, Mr. Hoekstra.

Mr. HOEKSTRA. Thank you, Mr. Chairman.

I just returned from a trip to Iraq and Afghanistan and talking to our intel folks and our military folks. It became clear—and this hearing bears it out—if this was a war that was going to be fought by the lawyers, we would have won a long time ago. We are fighting a war, and we are lawyering up the process.

But just a few questions, Mr. Baker. On October 25 of 2001, were you briefed in on this program?

Mr. BAKER. October 25, 2001, I don't remember. I was briefed in the latter part of 2001. I don't remember——

Mr. HOEKSTRA. I am just wondering—October 25, 2001 is when Porter Goss, Nancy Pelosi, Graham and Shelby were first briefed in and asked to participate and provide their feedback on the program.

So the second time that they were briefed, November 14, 2001, Porter Goss, Nancy Pelosi, Graham and Shelby, would you have been read into the program at that point in time?

Mr. BAKER. I believe it was in that time frame that I was read in, somewhere in that time frame, October, November.

Mr. HOEKSTRA. These folks—I will correct the record—Speaker Pelosi was briefed at least four times within the first year of the program as this program was being designed.

In your experience, is it unusual for—maybe you can't answer it, but would it be unusual for the Chair and the Ranking Members of the House Intelligence Committees to be briefed on and to consult with the executive branch on national security issues that might not be extensively throughout either the Congress or throughout the executive branch?

Mr. BAKER. My understanding is there are regular briefings for the Chair and Ranking, and sometimes staff directors on both sides, and that takes place on a fairly regular basis. I have attended some of those.

Mr. HOEKSTRA. Was that limited exposure in executive branch and in Congress?

Mr. BAKER. There are very few people that attend those.

Mr. HOEKSTRA. Thank you. You indicated that the Weinstein letter had a lot of merit and would have a lot of impact; is that correct?

Mr. BAKER. Certainly within the Department of Justice, the executive branch, I think it would carry a lot of weight. As I said, it is not an Attorney General opinion or Pelosi opinion.

Mr. HOEKSTRA. It wasn't——

Mr. BAKER. It is not an act of Congress or a ruling.

Mr. HOEKSTRA. Right. But the interpretation is there.

Mr. BAKER. It is binding, certainly, on the Department of Justice and on the executive branch.

Mr. HOEKSTRA. I think I would also like to submit for the record the letter that we just got on September 17 from the Office of Director of National Intelligence that responds to a letter, I think, or a request that we put in to him from Mr. Joel that talks about a number of issues, and he references the Weinstein letter a number of times.

The CHAIRMAN. Without objection.

[The information follows:]

OFFICE of the Director of National Intelligence
Washington, DC 20511

September 17, 2007

The Honorable Silvestre Reyes
Chairman
Permanent Select Committee
on Intelligence
House of Representatives
Washington, DC 20515

The Honorable Peter Hoekstra
Ranking Member
Permanent Select Committee
on Intelligence
House of Representatives
Washington, DC 20515

Dear Mr. Chairman and Representative Hoekstra:

I am writing this letter in response to a request from the Ranking Member of the House Permanent Select Committee on Intelligence. I appreciate this opportunity to describe the civil liberties and privacy protections that my office is charged with overseeing in the implementation of the Protect America Act of 2007.

Role of the Civil Liberties Protection Officer. I am the Civil Liberties Protection Officer for the Office of the Director of National Intelligence (ODNI). Congress has entrusted me with statutory responsibility to "ensure that the protection of civil liberties and privacy is appropriately incorporated in the policies and procedures" of the Intelligence Community. 50 U.S.C. § 403-3d(b)(1). As a result, my office is working closely with the Department of Justice and the DNI's Office of General Counsel, to help ensure that the intelligence agencies that implement the authorities under the Protect America Act have put in place adequate safeguards to protect the privacy and civil liberties of American citizens, legal residents, organizations and corporations ("U.S. persons"), as required by law and by the rules that have traditionally governed our intelligence activities. In addition, my office is working with the Department of Justice and DNI's Office of General Counsel to conduct formal, periodic assessments of compliance by agencies exercising authorities under the Protect America Act, and briefing the staffs of various congressional committees frequently and in depth.

The Larger Context - Protection of Civil Liberties and Privacy in the Intelligence Community. In order to understand the civil liberties and privacy protections that are being implemented under the Protect America Act, it is important to put the Act in the larger context of

how the Intelligence Community has historically protected information about Americans. As you know, intelligence agencies collect, retain, and disseminate information about U.S. persons. One of the limitations placed on the collection and use of U.S. person information is found in Executive Order 12333. That Executive Order provides that collection of intelligence is to be "pursued in a vigorous, innovative and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the Constitution was founded." It was signed by President Reagan in 1981, building on similar orders signed by Presidents Ford and Carter, to address the findings of the Church and Pike committee investigations of the mid-1970s. It put in place key restrictions on intelligence activities, sometimes referred to as "U.S. person rules," and has become part of the fabric of the Intelligence Community.

These rules – further detailed by procedures approved by the Attorney General for each agency – are not implemented in a vacuum. They are interpreted and applied by offices of general counsel at each intelligence agency, with compliance audited by offices of inspector general.[1] And of course, as you and the members of your committee are well aware, a critical outcome of the Church and Pike reports was the establishment of the House and Senate Intelligence Committees. Since the nature of intelligence by necessity requires secrecy, and therefore full transparency cannot be provided to the public at large, the Intelligence Committees, by exercising oversight over classified activities, can ensure that the Intelligence Community is protecting the nation from foreign threats while at the same time protecting our civil liberties.[2]

The Protect America Act. As Director McConnell and others have explained, as a result of technology changes in the global communications network, in recent years a substantial volume of communications of persons in foreign countries have been subject to the Foreign Intelligence Surveillance Act (FISA) despite Congress's intent in 1978 to exclude such activities. These changes resulted in applying the framework of probable cause and prior court review to foreign intelligence targets in foreign countries. In passing the Protect America Act, Congress changed the law to exempt from electronic surveillance "surveillance directed at a person reasonably believed to be located outside the United States" in order to obtain "significant foreign intelligence." As a result, probable cause and prior court review are not required for surveillance of foreign intelligence targets in foreign countries for foreign intelligence purposes.

Congress was concerned, however, with (1) whether the target of the surveillance is really in a foreign country, and (2) the privacy and civil liberties interests of U.S. persons who may be in communication with the target. To address these two issues, Congress required the Director of National Intelligence and the Attorney General to certify two separate sets of procedures with respect to acquisitions conducted under the Protect America Act:

---

[1] Violations of these rules are required to be reported to the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board. See Executive Order 12334 (Dec. 4, 1981) (establishment of Intelligence Oversight Board).

[2] Moreover, violations of law are required to be reported to the Intelligence Committees. See National Security Act of 1947, as amended, 50 U.S.C. § 413(b).

(1) reasonable procedures for determining that surveillance to be conducted pursuant to the Protect America Act concerns persons reasonably believed to be outside the United States ("foreign targeting procedures"), which must be reviewed by the FISA court, and

(2) minimization procedures that meet the definition of "minimization procedures" under FISA.[3]

In conjunction with the Department of Justice and the DNI's Office of General Counsel, we are focusing our oversight on ensuring that both sets of procedures adequately protect the privacy and civil liberties of U.S. persons, and that they are being followed by agencies of the Intelligence Community.

Is the target really a foreign intelligence target in a foreign country?

My office, the Department of Justice, and the DNI's Office of General Counsel has reviewed the foreign targeting procedures to ensure that they protect privacy and civil liberties, and is involved in reviewing their implementation to ensure that the procedures are followed. The statute does not require perfection, but it does require procedures that ensure collection is only undertaken against persons "reasonably believed to be outside the United States."

The need to perform this analysis is nothing new for the National Security Agency or other Intelligence Community agencies. Agencies have developed, over decades, policies and procedures to ensure that their monitoring activities did not inadvertently collect domestic information by mistake. However, in the Protect America Act, Congress went a step further, by requiring these procedures to be certified by the Director of National Intelligence and the Attorney General and submitted for review by the Foreign Intelligence Surveillance Court.

Significantly, the statute applies the foreign targeting procedures to "the acquisition of foreign intelligence information . . . ." As a result, the Intelligence Community's procedures for this kind of collection must enable analysts to determine, prior to obtaining any communications under the Protect America Act, that there is a reasonable belief that the target is a foreign intelligence target in a foreign country. Detailed procedures, which have already been submitted to the Foreign Intelligence Surveillance Court, explain how this is done. The procedures are classified because they discuss precisely how the Intelligence Community performs collections. However, I can describe them in general terms.

This "foreign targeting" determination that analysts must make may be relatively straightforward for certain forms of communication, and may be more complex for other forms of communication. The Intelligence Community uses a variety of sources of information, including technical analysis, information about the target from other intelligence reporting, and databases that are commercially available or otherwise lawfully obtained. Analysts are generally

[3] Section 105B of FISA, as amended by the Protect America Act, requires the Director of National Intelligence and the Attorney General to certify, among other things, that: "there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be outside the United States, and such procedures will be subject to review of the [FISA] Court . . ." and that "the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under [FISA]."

able to assess, with a high degree of confidence, whether a particular foreign intelligence target is in a foreign country. When they cannot do so, they will not initiate collection against that target.

While the procedures require this foreign targeting determination to be made prior to initiating collection, a variety of means are also employed to verify that the determination continues to be accurate after collection has begun. Even where the initial decision was correct, the location of the target may change. The Intelligence Community does not simply rest on its initial decision. Methods used to double-check the foreign targeting determination are employed frequently, even daily in some cases.

Questions have been raised about Americans traveling or residing abroad. Section 2.5 of Executive Order 12333 protects Americans – and U.S. persons generally – who may be encountered by the Intelligence Community overseas, by prohibiting the use of techniques that would require a warrant if used for law enforcement purposes, unless the Attorney General has determined that there is probable cause to believe the U.S. person is an agent of a foreign power. This requirement – in place since 1981 – has been judicially reviewed and upheld,[4] and is not affected by the Protect America Act. As a result, analysts must – and do – take steps to ensure that their "foreignness" determinations under the Protect America Act not only involve an assessment of the target's location, but also of whether the target may be a U.S. person. If the target is a U.S. person, collection may not be initiated without authorization under section 2.5 of Executive Order 12333, based on a finding of probable cause that the target is an agent of a foreign power.[5]

Questions have also been raised about "reverse targeting" – that is, could an intelligence agency target a person overseas as a pretext for intercepting the communications of the individuals inside the United States with whom the foreign person is in contact? The simple answer is that when the agency's actual purpose is to surveil the person in the United States, it must obtain a court order as required under FISA. This is also not a new problem for either the intelligence or law enforcement communities. When wiretapping the phone of any target – be it the NSA targeting a foreign terrorist or the FBI obtaining a law enforcement warrant to tap the phone of an organized crime figure – it is inevitable that conversations will be overheard with "incidental interceptees," individuals who are not the original targets but who might disclose information of interest.

The concerns about how to police this in practice are understandable, yet it is difficult to come up with a strict quantitative or other bright line test on such matters. You should rest assured that I intend to work closely with the Department of Justice, the DNI's Office of General Counsel, and the offices of general counsel of the agencies involved to develop further training and guidance in this area as needed, to safeguard against reverse targeting and protect privacy and civil liberties. It is important to recognize, also, that reverse targeting makes little sense as a

[4] In *United States v. Bin Laden*, 126 F. Supp. 2d 264, 277 (S.D.N.Y. 2000), the court "adopt[ed] the foreign intelligence exception to the warrant requirement for searches targeting foreign powers (or their agents) which are conducted abroad." See also *United States v. Duggan*, 743 F.2d 59, 71 (2d Cir. 1984) (citing cases); *United States v. Marzook*, 435 F. Supp. 2d 778 (E.D. Ill. 2006) (upholding 1993 physical search under section 2.5).

[5] The court in *United States v. Bin Laden*, 126 F. Supp. at 282 n.23, also noted that it did "not take issue with the policies and procedures" of section 2.5.

matter of intelligence tradecraft: if intelligence officers are indeed interested in a target inside the United States, they will have a natural incentive to seek a FISA court order in any event so as to obtain all of that person's communications, rather than the limited subset that would otherwise be acquired through such reverse targeting.

Are minimization procedures protecting the privacy and civil liberties of U.S. persons?

As discussed above, when the communications of persons overseas are acquired, it is inevitable that some of those communications will incidentally involve U.S. persons. Again, this is a familiar challenge for the Intelligence Community. In general, "minimization procedures" are procedures for reviewing, handling, and, as appropriate, destroying, information about U.S. persons, depending on whether or not the information constitutes foreign intelligence information or fits within another category the agency is authorized to retain. The FISA statute fully embraces and incorporates the concept of minimization as a way of dealing with the inevitability of incidentally intercepting communications of U.S. persons during authorized FISA surveillance.[6]

The Protect America Act requires that similar minimization procedures be followed with respect to surveillance conducted under the Act. These minimization procedures are intended to protect the privacy and civil liberties of U.S. persons who may be communicating with targets overseas. The Act requires that these procedures meet the definition of "minimization procedures" under FISA. My office, the Department of Justice, and the DNI's Office of General Counsel, have reviewed the minimization procedures, and, as part of our periodic compliance assessments, are reviewing compliance with those procedures. These procedures have been made available to the Intelligence Committees. Although not required by the Protect America Act, it should be noted that NSA is using minimization procedures previously reviewed and approved by the Foreign Intelligence Surveillance Court.

Because the minimization procedures used for the Protect America Act are themselves classified, it may be helpful in this unclassified letter to review those procedures for collecting, retaining, and disseminating U.S. person information in place at NSA, that have been released in

[6] FISA defines "minimization procedures" as:

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information; (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102(a), procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 105 is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

unclassified form. While these minimization procedures are not identical to the ones used for the Protect America Act, they provide general guidance for the types of processes and requirements involved with minimization.

United States Signals Intelligence Directive 18 (USSID 18) implements the requirements of Executive Order 12333 for the signals intelligence system. USSID 18 states plainly that "The Fourth Amendment to the United States Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. government." (§ 1.1). While some portions of the USSID are classified because they reveal sensitive sources and methods, most of it is unclassified and it has been periodically released under the Freedom of Information Act.[7] USSID 18 applies specific rules for retention, processing, and dissemination of any for communications that are to, from or about U.S. persons:

- Such communications may generally only be retained in raw form for a maximum of five years, unless there is a written finding that retention for a longer period is necessary to respond to a foreign intelligence requirement (§ 6.1.a(1));

- Intelligence reports from such communications are written "so as to focus solely on the activities of foreign entities and persons and their agents." (§ 7.1)

- Identities of U.S. persons are generally redacted from intelligence reports and replaced with generic terms such as "U.S. person" or "U.S. firm." Deleted identities are retained for a maximum of one year. (§ 7.1)

- U.S. person identities may generally be released only where the U.S. person has consented to such release, the information about the U.S. person is publicly available (e.g., a foreign target discussing a news report), or the identity of the U.S. person is necessary to understand foreign intelligence information or assess its importance (§ 7.2).

- The USSID lists specific responsibilities, including regular inspections, reports, legal reviews, and training for the Inspector General, General Counsel, and Deputy Director for Operations. Violations must be reported on a quarterly basis to the President's Foreign Intelligence Advisory Board through the Assistant to the Secretary of Defense for Intelligence Oversight. (§ 8).

USSID 18 also contains standard minimization procedures for surveillance conducted by NSA pursuant to the Foreign Intelligence Surveillance Act. These procedures supplement the standard USSID 18 procedures for all signals intelligence activities. They apply substantially the same process, with a few additional safeguards, notably that:

- The acquisition must be made in a manner "designed to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the surveillance." (App. 1. § 3(a)).

[7] A redacted version is available from the National Security Archive, a non-profit organization affiliated with George Washington University, at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-01.htm

- The lines or numbers being targeted must be verified as the lines or numbers authorized, and collection personnel must, at regular intervals, confirm "that the surveillance is not avoidably acquiring communications outside the authorized scope of the surveillance." (App. 1, § 3(b)).

In sum, the Protect America Act puts in place privacy and civil liberties protections (1) to help ensure the targets of surveillance are located outside the United States, and (2) to minimize information that is not necessary to understand foreign intelligence or assess its importance in communications to, from or about U.S. persons.

Other Questions

Questions have also been raised about other potential uses – and mis-uses –of authorities granted under the Protect America Act. On September 14, Assistant Attorney General Kenneth Wainstein explained why the Protect America Act does not authorize – among other things – reverse targeting, surveillance of domestic communications that merely "concern" a foreign target, physical searches of Americans' homes, effects or mail, or obtaining Americans' medical or library records. The oversight mechanisms outlined below will help ensure that the Protect America Act is being applied in a manner consistent with those interpretations.

Questions might also be raised as to whether the Protect America Act could enable the Intelligence Community to conduct surveillance for non-intelligence purposes. The requirement that surveillance under the Protect America Act be for "foreign intelligence" purposes also would prohibit abusing such authority for surveillance of Americans' political, religious, or any other domestic activities. Moreover, the provisions of Executive Order 12333 and each agency's Attorney General-approved procedures have for decades required that agencies demonstrate a valid mission-related purpose for collecting, retaining, or disseminating information about a U.S. person.

Other Offices and Institutions Involved in Oversight

While my office takes its oversight responsibilities very seriously, as discussed throughout this letter, it is not alone. As described in more detail in the September 5, 2007 letter of Principal Deputy Assistant Attorney General Brian Benczkowski, the Department of Justice, through the National Security Division, and the Director of National Intelligence, through my office and the DNI's Office of General Counsel, are conducting reviews of the implementation of the Protect America Act. These reviews started within 14 days of the initiation of collection under the Protect America Act and every 30 days thereafter. I am conducting these reviews together with the ODNI's Office of General Counsel and the National Security Division of the Department of Justice.

The following other offices and institutions, in all three branches of government, have a direct role in oversight of the Protect America Act – this list is not exhaustive:

Executive Branch, within the Intelligence Community:

- The Inspector General of the NSA conducts regular audits, inspections and reviews of compliance with USSID 18 and minimization procedures – it is also conducting an audit of the implementation of the Protect America Act;

- The General Counsel of the NSA provides legal advice and assistance and performs oversight in accordance with USSID 18 and the Protect America Act. It also helped develop the training courses on USSID 18 and the Protect America Act and supports administration of the training to the NSA workforce;

- The Signals Intelligence Directorate Oversight and Compliance Office provide oversight and compliance for the implementation of the Protect America Act at NSA;

- Other agency offices of general counsel and offices of inspector general perform similar oversight roles with respect to their agencies' use of this authority;

- The Office of General Counsel of the ODNI provides legal advice and assistance to the DNI in making his certifications under the Act, in assessing compliance with the procedures, an in reporting those assessments to Congress.

Executive Branch, outside the Intelligence Community:

- The Justice Department's National Security Division is conducting compliance assessments, as it does with respect to other FISA authorized activities;

- The Justice Department's National Security Division, the Office of Legal Policy and the Office of Legal Counsel are providing policy and legal advice with respect to the Protect America Act;

- The Justice Department's Civil Liberties and Privacy Office is consulting with the National Security Division in its assessments under the Protect America Act;

- The Privacy and Civil Liberties Oversight Board, currently within the Executive Office of the President, is conducting its own review of the policies and procedures of the Protect America Act;

- The Assistant Secretary of Defense for Intelligence Oversight reviews reports of violations by NSA, and other Defense Department intelligence entities, on a quarterly basis;

- The Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board receives reports of violations on a quarterly basis;

- The DoD Office of Inspector General also conducts regular audits, inspections and reviews of compliance with USSID 18 and minimization procedures.

Legislative Branch

- The Permanent Select Committee on Intelligence of the House of Representatives, and the Select Committee on Intelligence of the Senate are conducting intensive oversight of the Protect America Act.
- Members and staff have engaged in multiple oversight visits at the NSA;
- Both committees have held open and closed hearings on the subject, and have received numerous staff and member briefings.
- The House and Senate Judiciary Committees have likewise received oversight briefings, have conducted oversight visits, and have held public hearings.
- Congress will have an opportunity to revisit and clarify language in the Protect America Act before extending the Act or making it permanent.

Judicial Branch

- The Foreign Intelligence Surveillance Court has a direct role under the statute in reviewing procedures by which the Intelligence Community determine that a target is outside the United States.
- These procedures have already been submitted to the court and are currently under review.
- A recipient of a directive under section 105B of the Protect America Act may challenge its legality before the Foreign Intelligence Surveillance Court.

This extensive oversight helps ensure that agencies implementing the authorities of the Protect America Act are doing so in a careful, thoughtful, way that is fully transparent to the Congress, and that demonstrates due regard for the protection of privacy and civil liberties of Americans.

I hope this information is helpful. If you have any questions or would like more information on any of these issues, please contact Kathleen Turner in the Office of Legislative Affairs at (202) 201-1698.

Sincerely,

Alexander W. Joel

Mr. HOEKSTRA. Thank you, Mr. Chairman.

In the Weinstein letter, we ought to just be clear in the extent—you said you have not had an opportunity to study it or read it, correct?

Mr. BAKER. Correct.

Mr. HOEKSTRA. Here are parts of what that letter says.

In his interpretation, the Protect America Act leaves in place FISA's requirement for court orders to conduct electronic surveillance directed at persons in the United States.

So it does leave in the FISA restrictions. The Protect America Act does not authorize so-called domestic wire-tapping without a court order. He asked, in the letter it says, again quoting, "Does the act authorize physical searches of domestic mail, without court order, of the homes or businesses of foreign intelligence targets located in the United States, of the personal computers or hard drives of individuals in the United States? The answer to each of these questions is, no, the statute does not authorize these activities."

It goes on to say, "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."

I don't think it came up in the testimony of any of the witnesses, but, you know, one of the discussions that has been taking place over the last 6 weeks, again, with what I think, people just saying, I think it was Mr. Baker, you said people could construct an argument, you know, that would lead people to a different conclusion than what Mr. Weinstein says, but I think others have described it to us as being a very tortured argument to get there. Obviously Weinstein is not making that. But in terms of reverse targeting, here is the position of the Department of Justice: "It would remain a violation of FISA. The government cannot and will not use this authority to engage in reverse targeting."

I think your point is right on, because if you take a look at the letter from the DNI's office, is, they reference the judgments by the Department of Justice that they are putting in place the proper procedures and the rules to make sure that, you know, nobody in the Intelligence Community violates the interpretation.

Now, for the letter to come out from Justice, does Weinstein just kind of look at it and write it out? How extensively does this get vetted before it comes back to go to Congress?

Mr. BAKER. I would certainly hope, and it usually was the case in the past, that these kinds of letters are vetted very carefully within a variety of different offices inside the Department.

Mr. HOEKSTRA. Yes, it gets extensively reviewed. I think that is one of the frustrations sometimes we have with the executive branch, that to get anything out of the executive branch, just about anybody who tangentially touches it has a say in it before it is completed.

Mr. BAKER. I would also expect, I am sorry, that it would have been vetted through the Intelligence Community as well.

Mr. HOEKSTRA. Would career staffers have reviewed this document as well, typically?

Mr. BAKER. I don't want to overstate what I know about the provenance of this document. I just don't know. Normally, at least when I was there, I was called upon to read a variety of different letters and statements over time; statements, people coming up to Congress and so on. I have been gone for the past 9 months, though, so I don't want to overstate what I know personally.

Mr. HOEKSTRA. You also testified that FISA provided timely and actual intelligence when requested. You also used some words that, you know, "it takes a little time," I wrote down. I don't know what exactly your words were, but I think it was something like it goes really fast when everything is ready.

What does that mean, "everything ready"?

Mr. BAKER. Well, I have been thinking about that during the break, Mr. Hoekstra. As I testified, when you were Chairman, I testified about this process at length, and I think it took us a while, I think, actually to get through and for me to give a full and complete—what I believe at the time was a full and complete explanation of how the emergency process works.

The emergency process, there are complications to it. I don't mean to sit here today that you push a button, or it is not like click "buy now" on the Internet. It does take time.

So the Intelligence Community has to do their investigation, make a judgment about what targets they want to pursue. When they have done that, and when they have reached a point where they realize that they need to do collection immediately, they start talking to us.

Then we work through the legal facts, the legal issues, the factual issues, at the same time that they are dealing with the technical stuff that they need to do. Then when all that is ready and they tell us we are ready to go, and they say, "Yes, we resolved all legal issues, we have no problem, call the Attorney General," calling the Attorney General and getting an answer back, that is not like super time-intensive, unless it is a complicated case.

Oftentimes we will go down and prebrief the Attorney General what the case is all about, what the request will be, so that when the call comes it can happen quickly.

Mr. HOEKSTRA. I think that is the reason I came back to this is, I don't specifically remember your testimony, but I agree, the Justice Department can put in approval processes that are very quick, because you have got a number of people that can approve these emergencies. It is a phone call, you can do the prebriefing, and so when you finally get the 1- or 2-inch packet of information that the Justice Department attorneys have worked on with the Intelligence Community, it is kind of like, yes, it is done, you know it is coming and those types of things, but there may be extensive work required to get to that point.

Mr. BAKER. That is what I tried to suggest in my opening remarks, because none of this is easy, none of this is cost-free. There are lots of people working all the time, and have been for lots of years, on this stuff. We have done everything we can to expedite it. These things are posted on a secure Web site. We look at them.

There is lots of things posted and back and forth on the Intelligence Community, so everybody on both sides, DOJ and the Com-

munity, worked really, really hard to cut out unnecessary steps and unnecessary delays.

Mr. HOEKSTRA. When you go through that process, the first part takes some time. I think that is probably why the current Speaker and others in the congressional community, along with the folks in the executive branch, decided that with the threat that they faced in 2001, the threat that we continually face, speed is an option. And it is not always getting all of that information done—is not necessarily the most effective way in dealing with the issue.

I think we have had someone who comes in with the FISA applications, who said that, you know, quite often, in the Intel Community, taking 2 weeks to prepare and get the package ready is not unheard of. It is probably more of what the time typically takes.

Mr. BAKER. My answer to that is we are constantly prioritizing our work based on what the Intelligence Community needs. So the things that they need first and they tell us they need first we do those first. Or they did when I was there.

Second, as I suggested, it is not unlimited resources, and what jumps in front of the line is going to push other things back. So sometimes the folks working on those other cases don't understand exactly that other things have jumped ahead. They can get frustrated—we know that—and they can try to deal with it.

Mr. HOEKSTRA. It can be difficult, because I am assuming you believe that the threat is not just Afghanistan-based, it is not just Pakistan-based, it is not just Iraq. There are other places out there. We just had the takedown of a threat in Germany; Denmark, a year ago. We had the threat out of the U.K. For a lot of these streams or threat streams, you don't necessarily know which one is the priority, and there is a lot of uncertainty associated with each of these.

You also testified, and I think you have helped clarify that, exactly how the FISA process worked, because obviously not everybody necessarily agreed that it was—I think you have just said the same thing—it is not necessarily fast and agile.

Are you aware of any comments of General Hayden, who was at that time the head of NSA, any comments that he might have made about the FISA process and the statements that he would have made publicly?

Mr. BAKER. I can't remember specifically. I know General Hayden has spoken about these issues. I can't remember a specific statement about that. It wouldn't surprise me that he commented on that though.

Mr. HOEKSTRA. There are others within the Intelligence Community, when they looked at the threat, when they looked at the kinds of folks we are facing in these types of things, that, you know, they reached the conclusion that the FISA process wasn't working.

I think that is the case that, you know, General Hayden made to the political leaders in the executive branch. But that is also the argument that he made to the congressional leadership back in 2001, saying that, you know, with the kind of threat that we have out there, it just doesn't work. I think that is why for 4 years, until The New York Times reported the existence of the program, the congressional leadership supported this.

Mr. Rivkin, during your experience in the executive branch, what was your experience with FISA?

Mr. RIVKIN. Well, Congressman, I was like Peter, I have not been involved in individual applications, but I have been involved in the White House Counsel's Office, my days at Justice, the general intelligence policy issues. My view, frankly, is the whole debate about how rapidly the system can move is not the biggest problem, because you can give more resources, you are going to have 20 emergency applications going forward.

The problem is, in my opinion, quite different. The problem is, if you are going to go for warrants, you limit dramatically the range of circumstances where you wouldn't even bother getting an application going. Because, look, I actually believe that war means something real; it is not just it is a good idea to go.

There is a whole range of scenarios where you cannot get a warrant, because the individual involved is not guilty of anything. Not only the person, not a member of al-Qa'ida, or an al-Qa'ida sympathizer, he may just be an independent bystander who happens to have information about a person who is a relative of a member of al-Qa'ida that you might want to get.

Remember, in all those emergency situations, you basically have to convince the Attorney General that he can attest that warrant—or, excuse me, warrant would be attainable. There are many circumstances where you just cannot do it. You are missing, you are really focusing, you are drilling down on a portion of the spectrum of warrants that can be issued, and you are overlooking the ones that cannot.

Mr. HOEKSTRA. It is very similar to when I first joined the Intelligence Committee and started talking with the folks out in the field about the chilling effect of the Deutsche doctrine. I don't know if you are familiar with the Deutsche doctrine, back in 1996, where then-President Clinton said we really don't want to recruit people with criminal or human rights violations, and the end result is that it had a chilling effect on all types of collections.

Mr. RIVKIN. That is a perfect analogy. You are arbitrarily, in a wholesale fashion, dismissing the whole range of collection, a portion of collection that could have been useful.

Mr. HOEKSTRA. Thank you.

The CHAIRMAN. Thank you, Mr. Hoekstra.

I wanted to make a couple of points.

Mr. Baker, the letter that Mr. Hoekstra was referring to, that with the new Attorney General coming in, could he have that letter pulled and substitute something else for you?

Mr. BAKER. Since it is an interpretation of the Department, somebody at Mr. Weinstein's level or higher is going to have to reverse it. It could be the next Attorney General, it could be anybody, but they are going to have to do it. They are going to have to then, it seems to me, explain—the new folks would have to explain why it is that they are not going along with the interpretation set forth in the letter that we are talking about.

The CHAIRMAN. So it could be pulled?

Mr. BAKER. I guess, Mr. Chairman, the way I read it is it is binding on the executive branch today. It is not binding for all time.

The CHAIRMAN. The other issue that I want to mention briefly, and then I want to ask a few questions as it relates to the Ranking Member's comments, is that I just wanted the record to reflect that the case that was just made in Germany and Denmark was made under the old FISA law, in fact. So if anybody says that FISA doesn't work, I would refer them to the latest case that was done by FISA.

Thank you, Mr. Baker.

Mr. Dempsey and Ms. Graves, what do you believe are the biggest flaws in the administration's bill or the PAA?

Mr. DEMPSEY. I think the biggest flaw is the lack of any reasonable checks and balances. We are trying to develop here a balanced system that provides the speed and agility that the intelligence agencies need, but at the same time provide some form of oversight.

Under the Protect America Act, there really is no role for the judicial branch of government.

There is a court order approving the procedures. It comes after the fact. It has no compulsory power, it is only on a clearly erroneous standard.

There is no after-the-fact review even of how the order is then implemented, about how the program is implemented.

I think that we can do a lot better to preserve the speed and agility to get the intelligence in a timely fashion, but also to make sure that the program is being properly implemented and the judicial branch under our system has a critical role in that, and that is lacking from the Protect America Act.

Ms. GRAVES. I would add that it is very clear to us that it allows warrantless secret searches of American communications without any after-the-fact or meaningful review. It eliminates prior judicial authorization and subsequent judicial authorization. It requires no individualized determination of probable cause for the Americans involved.

It requires no specification of the individuals or the phone lines that are to be surveilled. It also may have an impact on the use of this material in subsequent criminal prosecutions. It allows access, notwithstanding the statements of Mr. Weinstein, to stored communications records, which are the content of your e-mails and phone calls, that are stored by Internet search providers and telephone companies, with no court orders or judicial oversight.

The pen register rules are affected as well, and in that regard it allows the government to secretly retain the call record information and other revealing data on thousands or millions of American communications, with no judicial oversight to conduct traffic analysis and create maps of the associations and contacts of untold numbers of Americans.

It utterly lacks meaningful, independent oversight either for the courts or this body.

The CHAIRMAN. If we revise the new act, what are the most important provisions for us to modify, Mr. Dempsey and Ms. Graves?

Mr. DEMPSEY. I think that at the initial stage, the court review should be more probing than the review provided in the Protect America Act. That is not specific targeting. We are not talking here about giving the court, in the first instance, prior control or prior

approval over specific selection of targets overseas, but, instead, a review of the mechanism by which the government picks and chooses among which communications with Americans will be intercepted. And, then, secondly, a process of reporting back to the court, sort of like a traditional return on service or, like currently occurs under FISA, a report back to the court periodically about how the program is being implemented so that the court and the administration can determine when a particularized order is necessary, if it becomes clear that a particular American or an American is being affected.

So it is both somewhat more stringent prior review and then ongoing monitoring by the court of the implementation of the program. Both of those are lacking from the PAA.

Ms. GRAVES. I would suggest that the starting point would be H.R. 3356 with additional critical protection for Americans' communications, including individualized court orders before the fact or after the fact, and additional mandatory oversight by Congress, not optional, of significant things, including the number of Americans affected.

In addition, I would say that I think it is virtually impossible to fix the PAA, because it has utterly supplanted the structure of FISA and the definitions of electronic surveillance which are the key in FISA to when the warrant requirement kicks in.

We believe that surveillance must be carried out within the FISA structure. There should not be any change to the definition of electronic surveillance. We believe that the carriers must have responsibility for sorting the communications and ensuring that the NSA is given access to what they are entitled to. Not everything. Initial individualized court authorization is essential to any access to U.S. switches.

We believe that when the government intentionally acquires the communications of persons in the U.S., not targeting, intentionally acquiring communications of persons in the U.S., that they need to have court oversight; and that we believe that there must be limited exceptions, but more flexibility for true emergencies and additional resources that are utterly lacking in the PAA that are represented in previous versions that have been proposed by Democratic members of this committee.

We also think that it is essential that there be meaningful, mandatory and frequent reports to Congress, and the courts with an IG audit required on a regular basis; in particular, with a focus on the number of Americans whose communications are being swept in, even under a revised regime.

The CHAIRMAN. Also, Mr. Dempsey and Ms. Graves, do you believe that Congress should pass permanent changes to FISA before this current act sunsets next year?

Mr. DEMPSEY. Mr. Chairman, I really think you are going to have to take your time on this. I am not saying that the PAA should expire. I think that the Speaker has put you on a very tight time frame.

I think there are a lot of unanswered questions here. I don't think that the PAA, the Protect America Act, is a good starting point. I think there are some fundamental flaws in the way the statute works, and you have to have a five-page letter from Mr.

Wainstein saying what it does and doesn't mean: use of terms like "directed at" that aren't defined, and "concerning;" the whole notion of trying to do this by carving something out of the definition of "electronic surveillance" and then creating a procedure for things that are not electronic surveillance.

It is a very, very confusing statute, I think, to get this right, to respond to the technological changes that have occurred, to truly meet those core criteria of the DNI, also addressing the security problem. Now is this really a huge question: how is this being implemented in the telecommunications networks, and are we creating a certain risk of vulnerability by changes that might be made in the communications networks to cooperate with this?

So there are a lot of issues that the committee is going to have to go through here. I am not sure that it is going to be possible to put a few little things on the PAA.

I think that H.R. 3356 is a starting point for a proceeding here.

At the end of the day, though, it may be that the issues can not be fully resolved in this Congress. Honestly, there may have to be an extension of the Protect America Act and not a permanent authorization of it to give it more time.

We still don't have those court orders, so we are still not really sure what is the problem that we are trying to fix.

The CHAIRMAN. Ms. Graves.

Ms. GRAVES. I would say that it definitely should not be made permanent. The PAA should not be made permanent. We believe that the Congress should start by obtaining the information of past surveillance activities that many Members of this Congress believe are in violation of the law; obtaining legal opinions, not just the letters, of current assistant attorney generals. And as a former deputy attorney general, I can certainly tell you that my AAG's opinions didn't stand in the next administration, and wouldn't have stood, necessarily, for the next AAG.

But I would say that it is critically important that not only Congress have key information that you are entitled to. If the Department of Justice can do a white paper on its legal views, it can certainly share it OLC opinions, thousands of which have been shared with Congress in history, including many legal opinions during the Reagan administration, I would point out.

But beyond that, I would say that it is critically important that you and the American people have a certain amount of information about what happened and about the effect on Americans, because we don't they think that it is possible to have this debate, and permanently change the structure of FISA, revisit or revise the fundamental determination of Congress about the constitutionality of requiring warrants in this area without that information.

The CHAIRMAN. Thank you. Finally, what do you two think are the essential protections that we should have in any FISA legislation?

Mr. DEMPSEY. I think the key standard has to be that of checks and balances and creating the system of flexibility, speed and agility, but at the same time having all three branches of government involved in the oversight of this. Minimization is part of the answer, but only part of the answer.

Minimization overseen by a court is far better than minimization in the sole discretion of the executive branch. The Protect America Act leaves the definition or the drafting of minimization rules and their implementation solely to the executive branch.

I think the key guiding concept here is a workable system of checks and balances, starting with some kind of court approval for a program, and then followed by court supervision of that program.

You clearly have to address the immunity issue. I think companies should have immunity for cooperating with lawful surveillance, but I think the statute is meaningless if it can be ignored and if people can expect retroactive immunity for activity outside of the structure of the legislation.

Otherwise, what are we doing here? We are passing a law that can be ignored. Even if the Protect America Act were completely renewed in its splendor, if we then give the companies retroactive immunity, a future Attorney General can go outside even of the PAA, and the companies might expect that they would be granted retroactive immunity for that as well.

I don't think it should be ruinous liability. I think that needs to be addressed. We need to find some way to make sure there is a consequence, but clearly no one wants to put phone companies out of business.

Ms. GRAVES. I would say that in addition to the points I mentioned about the structure of FISA and preserving individual warrants, that clarity is absolutely essential. We have great respect for the NSA linguists, analysts and technicians who are doing their job every day to keep the country safe.

But their job is to collect against requirements. When those requirements are ambiguous and overly broad and increase the effect on American communications, we need tighter rules, better rules, with flexibility but not limitless elasticity, which is what the PAA involves.

We think that the mandatory oversight by the courts, before the fact or after the fact, and mandatory reporting to every member of this committee—not selectively, not when the administration wants something and they need to give you something before they are going to testify, but mandatory and regular reporting of this committee—is essential.

The CHAIRMAN. Very good, thank you. Mr. Hoekstra.

Mr. HOEKSTRA. Thank you, Mr. Chairman.

Mr. Rivkin, are you familiar with the case of the Supreme Court, the United States v. Verdugo?

Mr. RIVKIN. Yes.

Mr. HOEKSTRA. I find it interesting, I just want to pursue this a little closer. What I find here is that we have got people who are at least alluding to the fact that we ought to be extending fourth amendment protections to foreign individuals, non-U.S. citizens outside of the United States. What Verdugo says is we think that the text of the fourth amendment, its history and our cases, discussing the application of the Constitution to aliens and extraterritorials, requires rejection of the respondent's claim. At the time of the search he was a citizen and resident of Mexico, with no voluntarily attachment to the United States, and the place

searched was located in Mexico. Under these circumstances, the fourth amendment has no application.

It also goes on: Application of the fourth amendment to those circumstances could significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest. I think the Supreme Court has pretty clearly identified that.

If we take a look at where some want to go in applying the protections of the fourth amendment to foreign individuals, I think you alluded to this a little bit on targeting. In a criminal case, if I have been targeted in the United States, and there is a warrant against me, or a warrant enabling me to be surveilled, if my child's teacher calls me today, is that going to be listened to?

Mr. RIVKIN. Of course. And any number of individuals who call you, whom you contact.

Mr. HOEKSTRA. Earlier today someone said, well, you know, we know who is calling, we ought to know. We have the opportunity to go through that.

That is not true. You call a number, and it may be located—you are calling from Afghanistan, and you may be calling from what you think is a cell phone that at that point in time may be located in Germany, but you don't know who is going to answer it. You don't know who is going to be on the other end of the line, and you are not really sure, and you are not going to be positive as to where it is going to be located; so it is the same kind of thing. Isn't that correct?

Mr. RIVKIN. That is absolutely correct. I know a number of people, I have a good friend who used to be a foreign Ambassador. He got a mobile phone with area code 202 because enough people remember it. A person has been gone for 8 years and still uses the same area code.

When I get a call from him, and it registers on my mobile phone, it says 202, I don't know if he is calling from Germany or if he is in New York. All the notions about you know how to reach the phone number, I mean, unless we are in science fiction mode, you do know which phone number you are calling. But you have no idea, just by looking at that number, where that person is. You think frequently you have to look at the conversation's content to realize that person is near Lake Cuomo and not Lake Wobegon.

Mr. HOEKSTRA. So it is very difficult, it is impossible to design a fail-safe system. I am assuming that, you know, they say—for those that would argue and say, you know, get a FISA, under a FISA, there would be other Americans that would be listened to; is that correct?

Mr. RIVKIN. That is absolutely correct. Quite frankly, again, it is difficult. We need to have somewhat more transparency, no pun intended, in this discussion. I suspect, I could be wrong, that the reason people are talking about putting most of the surveillance of overseas targets under warrant is because they know it would shrink the intelligence stream.

As I said in my prepared remarks, let's assume there is a relationship in the number of foreigners you surveil and number of Americans; what is the ratio. If you surveil 1 million foreigners, you are going to capture a big chunk of American communications.

If you surveil one-tenth of that, you would only capture one-tenth of a chunk.

So I think when people who want to protect the privacy of innocent Americans, quote, unquote, are really talking about reducing the number of foreign targets, which is a stunning situation, the first time in the history of this type of a statute we are talking about deliberately limiting the quantity and quality of our collection. That is absolutely stunning.

We have to be—because, look, if we do not diminish the number of foreigners we listen to, the fact that they are being listened to under warrant does precious little to protect the privacy of Americans who get caught by virtue of being communicated by that person.

The privacy of persons is being affected by minimization, by oversight. What difference does it makes to you, Congressman, if you get a call from somebody who is being surveilled under warrant versus somebody who is not being surveilled under warrant, as long as their conversation is being listened to by virtue of the targeting being done by that person? Makes no difference. Wouldn't make any difference to me.

Mr. HOEKSTRA. The incidental collection of U.S. citizens, did this start under the terrorist surveillance program?

Mr. RIVKIN. Of course not.

Mr. HOEKSTRA. Did it start, you know, under FISA in 1978, 1978, 1979 when that originally passed?

Mr. RIVKIN. No, I don't think—and as I mentioned in my prepared remarks, Congressman, incidental collection is an inevitable attribute of any kind of collection of information of guilty parties. Let's face it, guilty parties don't only call other guilty parties. Even gangsters don't call only other gangsters.

If you are going to surveil anybody or listen to anybody, using whatever technical means, you are going to capture a lot of innocent people. That goes—in my opinion, dates back to the dawn of times when you started surveilling people.

Mr. HOEKSTRA. The terrorist surveillance program as it is developed, is this legislation that we passed a couple of months ago. When Speaker Pelosi is reviewing this process and deciding in 2001 and in 2002 that this is something that we ought to be going ahead with, she is consulting with the administration they would have had in 2001. At least under FISA, they would have had 23 years of experience in review of the Intelligence Community as to how the Intelligence Community dealt with incidental collection of U.S. citizens; isn't that correct?

Mr. RIVKIN. That is absolutely correct. Not being involved in oversight from, certainly, a legislative perspective, it is difficult for me to be definitive as to what should be augmented. Let me put it generally, because this is an excellent question. We should have a serious debate about how to control the consequences of collection. There may be more that needs to be done to minimization. There may be need for more oversight. Again, if it were up to me, maybe you need to broaden it beyond the gang of eight.

What is untenable in my opinion is deliberately limiting the collection because you worry about the consequence of collecting something. It is like the collective closing of your eyes and then plugging

your ears. That is an absolutely—in the world, when the 9/11 Commission talks about connecting the dots and removing the impediments, that is such a stunning reversal of policy that makes sense.

Mr. DEMPSEY. Congressman, could I contribute to this?

Mr. HOEKSTRA. You have had plenty of time, all right. I appreciate your input, but I would like to get the other side of the story on the record as we go through it as well today.

I don't believe that in the roughly 30 minutes of questioning by the other side of the aisle that Mr. Rivkin was ever allowed the opportunity to answer or provide any feedback or any response to that. At least I have had the opportunity to question both Mr. Baker and Mr. Rivkin on the issues that have been in front of us.

I am going to go back to Mr. Baker.

There were discussions earlier debating the legality of the terrorist surveillance program, citing a book by Mr. Goldsmith. The Attorney General has publicly stated that the activities previously conducted under the terrorist surveillance program have been moved under orders of the FISA court.

In doing so, would Federal judges have found that the activities they authorize were lawful?

Mr. BAKER. I am sorry, Congressman, can you repeat?

Mr. HOEKSTRA. The Attorney General has publicly stated that the activities previously conducted under the terrorist surveillance program have been moved under orders of the FISA court.

And doing so, Federal judges found the activities they authorized were lawful.

Mr. BAKER. I don't believe I can comment on the substance of the orders from January. I guess that is maybe all I can say right now. I mean, those haven't been disclosed, so I don't believe I can comment on what the court was doing in January.

Mr. HOEKSTRA. Mr. Chairman, with that, I will yield back my time.

Thank you.

The CHAIRMAN. Thank you, Mr. Hoekstra.

I don't believe I heard anybody say that we wanted to extend Fourth Amendment rights to foreigners. I know I didn't hear any of the panelists, but I wanted to now start the Members' questions.

We will have a second round, so I would ask all Members to please respect the 5-minute rule, and with that, we will start with Ms. Eshoo.

Ms. ESHOO. Thank you, Mr. Chairman, for having this important hearing and to all of the witnesses. I think that this has really been enlightening and a very good forum.

Having said that, Mr. Rivkin, I am not so sure I understand your point. What I am taking away from what you said is that privacy rights are really not all they are cracked up to be or that some should have them or when we say "all" we really don't mean "all." I don't know what your succinct point is about the legislation that was passed on a hurried basis and that many of us have deep concerns about and so do the American people.

So I will get back to you so maybe you want to think about a couple of sentences that might just kind of knock your position, the ball out of the park. I am saying it respectfully. I didn't get what your point was.

Now I think that this is on the one hand, a somewhat complicated issue, FISA; it is complicated even more because there is secrecy involved. So when the American people hear any of us trying to explain not only what the law covers but how it functions or did function, they don't really feel like they are getting all of it. But when it comes to our rights, to our liberties and our national security, they really insist on both and both they should.

There isn't any small reason why both of those are covered in the oath that every single one of us takes when we are sworn into the Congress, that we swear to uphold the Constitution of the United States and to protect our Nation against all enemies, foreign and domestic.

And in my view, this is not a multiple choice test. We are obligated, the duties that we have and the oath that we take, to accomplish both. And I think that FISA is a very good example of this.

Now what are we struggling over? We seem to be struggling over a legal framework, a framework that actually is workable so that the Intelligence Community can do what it needs to do, that it has the tools that it needs but that we have a legal framework and that we have checks and balances.

In a secret undertaking, it is even that much more important to have checks and balances. And I think taking Harry Truman's statements, I think when it comes to that, the buck stops with us.

Is it any coincidence that the administration has refused to even hand over what the ranking member and the chairman of the committee have requested almost ad nauseam and they don't give it to us?

So how are the American people going to be protected and guaranteed not only of their liberties but also the absolute best on our part to secure our Nation?

So it is in that context that I want to ask the following question: Oversight is a word that I think is batted around but not fully appreciated. It really represents a lot.

So, to Mr. Dempsey and Ms. Graves, and if there is anybody else that wants to chime in, all four of you, what information do you think the administration should provide to Congress to ensure effective oversight?

And relative to these new authorities, they are essentially saying, "trust us". And you know what? I am not going to trust anybody with that. I want the information and be able to verify, and then I will trust. I am not going to throw trust away and just assume that it is going to be regarded.

Do you think that there should be an audit which includes a review of all of the directives that are issued pursuant to the new authority?

We don't have that now, and I would also like to hear, if we have time, about the information that you think that the administration is providing to Congress. Do you think it is effective enough today to allow us to do the oversight that I spoke of and not this, just this little word that seems to be cast about just because we are sitting here? You can't do oversight unless you get effective information in my view.

So we want to start with Mr. Dempsey.

The CHAIRMAN. Okay. Her time is up. So I will allow one of you to answer each one of the questions. I want to tell the Members, I have just been informed that we are going to have to give up the room at 1:25. So this will probably give us enough time for everybody that is here. But if you will quickly, each one of you, answer the questions.

Mr. DEMPSEY. I think that Congress does need to have access to the legal interpretations of the administration, not just to be orally briefed on things but to actually see the details about how these interpretations are being spelled out.

On the other hand, though, I don't think Congress should be in a position of receiving information about targeting, and I am not sure that Congress should be in the position of receiving a lot of information about how the program is being implemented in terms of we are intercepting this person or that person. That is why I think that the court has to be a part of this. I think that the court is a smaller entity. It has, I think, somewhat tighter processes, even than Congress has.

So you need both branches of government: Congress on the law; the court on some of these details.

Ms. GRACE. I would say that you definitely need the legal opinions of the Office of Legal Counsel for the entirety of this program in its various iterations from the beginning, whether that is the Comey pieces, before or after all those pieces you are entitled to them.

With respect to actual orders of the court, I think you are entitled to see some of those orders. And with regard to orders of the magnitude, what we believe was authorized earlier this year, you should see the applications because it is possible that the orders themselves may be very short and not allow you sufficient information to understand the arguments that were made, whether those arguments include the suggestion that FISA is not the exclusive means or that the President has the inherent ability to bypass FISA. You should know that before passing any permanent changes to FISA.

Mr. RIVKIN. My view is almost exactly the reverse.

The CHAIRMAN. If you can do it quickly.

Mr. RIVKIN. I happen to think you have to take the courts as you find it. The judiciary role is very narrow. They can deal with warrants. They are certainly not Article III courts. You, on the other hand, have enormous opportunity and an obligation to participate in the most intrusive oversight.

If it were to up to me to restore the sort of political sustainability of the program, I would be prepared to bring everybody in and have you do nothing but review applications on a daily basis as long as it is clear that you are doing it in your oversight capacity.

And if you feel as a Member that something fundamentally flawed is being done, if somebody is being surveilled and you happen to believe that this is a witch hunt, you know, you have reason to weigh cause and come to a legal position where you can disclose a summation of law and survive criminal prosecution. It is a responsible way of doing things. Trying to throw it to the court does not work.

Briefly on the legal opinions, there is a variety of reasons why you do not have any reason to see legal opinions. So long as you understand what was done on a practical level, getting legal opinions impinges in a fundamental way on the President's ability to receive confidential legal advice, particularly in the current atmosphere would do nothing more than chill a future President's ability to get legal advice. And it is absolutely not essential to your ability to create new regulatory structure.

Look at the actual behavior, not the legal opinions.

The CHAIRMAN. Mr. McHugh.

Ms. ESHOO. Mr. Baker had his hand up. He wanted to respond.

Mr. MCHUGH. Thank you, Mr. Chairman.

I will go to Mr. Baker.

Mr. Baker, we have had in other sessions Assistant General Comey, former Attorney General Ashcroft, Gonzalez and others have spoken to this, so I want to make sure that I understand your testimony.

When we are dealing with an emergency FISA application, is there a different standard that is employed as to the approval of that emergency application, one that is different from probable cause? Because that has not been my understanding. It is still the same standard, correct?

Mr. BAKER. The same standard applies.

Mr. MCHUGH. So if you were, whoever was in that acting role, you have to see an application that embodies in the basic tenants, all of the evidence, all of the record, all of the background that a FISA court would expect to see to create or to equal probable cause; is that true?

Mr. BAKER. I wouldn't agree with that.

I mean, there is no application at that point in time because the emergencies come in and we can make these things—it can be done entirely orally. It is not usually done entirely orally. But it can be. You could get a phone call from an intelligence agency that makes its way through the process to you. You can explain what is going on and you call the attorney general. But there usually is paperwork in there somewhere, but it is not usually a full-blown FISA application. That is what we work on.

Mr. MCHUGH. I didn't use the words "full-blown FISA application." What I said was it would have to embody much of the background, et cetera. That is what we have been told. Do you disagree with that?

Mr. BAKER. It has to have probable cause.

Mr. MCHUGH. Thank you. That is really the crux of the question.

Mr. Rivkin, you made the comment to the ranking member that if he were a target under a surveillance order here in the United States and his child's teacher called him, that that conversation would be subject to surveillance.

Would you agree with that, Mr. Baker?

Mr. BAKER. I thought you were asking Mr. Rivkin something.

Could you repeat the question?

Mr. MCHUGH. Yes. The question that the chairman posed or the former chairman posed to Mr. Rivkin said that if he, Mr. Hoekstra, were the target of a surveillance order here as a United States cit-

izen and his child's teacher called him, that conversation from that teacher would be subject to surveillance.

Mr. BAKER. It would be intercepted, yes.

Mr. MCHUGH. Mr. Rivkin, Ms. Graves said in her comments that we perhaps should not lend too much deference to the judicial record that has traditionally found that the executive has pretty broad latitude in issues of foreign intelligence because, as she put it, the courts are weak.

Would you argue the courts are weak or that the court cases have been pretty clear and consistent?

Mr. RIVKIN. I would say two things, Congressman. I think that the courts have acted to appropriate constitutional humility in this area because the executive has a greet deal of powers relative to national security, and the courts' powers are fairly narrow. But to the extent the courts have reached the merits of those issues—and probably the best summation of that case law is in the court of FISA, court of the review—they were very emphatic that the President, of course, has the power to gather intelligence in this field.

I would say more so in the time of war. It is really a species of battlefield intelligence not just foreign intelligence.

Mr. MCHUGH. Ms. Graves, one of the key issues here is a matter of what we are able to identify as a domestic call and what we are not. And you spoke to that in your testimony.

The phrasing you used was that, quote, it seems to me, end quote, I take it meaning your organization, that you ought to be able to identify that.

Testimony has been received previously that while in some cases it can be, in any number of cases it can't be, I am just curious, do you have a technical, professional opinion that shows we can't identify it in all cases because if we can, obviously that takes away a big part of the debate.

Ms. GRAVES. I tried to be very careful about the fact that we believed that in most and many instances that information can be ascertained, particularly with regard to phone calls.

But we do believe that it is important for this committee to hear from people with technology expertise beyond the government which has a particular perspective, and we also think that, to the extent that there are some calls where you don't know, the assumption shouldn't be, therefore, you get everything. There should be a way to categorize this that deals with the calls you do know and those that you don't having different presumptions and different rules with court involvement. We think that is important.

Mr. MCHUGH. But minimization procedure that deals directly with identifiable calls.

Ms. GRAVES. I am not sure I agree——

Mr. MCHUGH. The minute I said that, I thought, she probably doesn't like that phrase.

Some process by which we accommodate more definitively those calls you can't identify.

Ms. GRAVES. I would say it is important to have more court oversight, especially because more American communications are in this communications stream.

The CHAIRMAN. Thank you.

Mr. Tierney.

Mr. TIERNEY. Mr. Dempsey, the Ranking Member seems to be laboring over some misconception that somebody is promoting the concept of getting a warrant for foreign-to-foreign conversations.

Have you heard any of the witnesses today mention that that is something they put forward?

Mr. DEMPSEY. No. There has long been agreement that foreign-to-foreign should be exempted. I haven't heard anybody say that foreigners should be entitled to Fourth Amendment rights either. I am not saying that.

I think we are talking here about a situation. We used the hypothetical that the ranking member raised or Mr. Rivkin was discussing which was, if you have a target to—if you are targeting a person, you are targeting the school teacher and the school teacher calls you, should you care if your communications are intercepted? Well, if your communications are intercepted without a warrant, even if you are not the target, you still have a Fourth Amendment right and you have the right to object to that surveillance if the evidence is going to be used against you.

There was an interesting Supreme Court case where the Government was targeting a suspected drug dealer. They searched his mother's home. They weren't trying to investigate or prosecute the mother.

Well, it was held that even though the drug dealer was the target, his Fourth Amendment rights were not intruded upon. The Fourth Amendment rights that were at stake were the rights of the person who was being searched.

And in this case here, where you have two people being searched, people on both ends of the communication, it makes a world of difference whether there is a court order or not. The fact that you are not the target, if you are being intercepted without a court order, the fact that you are not the target makes no difference to the Fourth Amendment analysis. Your rights are being violated, and you have a right to object.

Mr. TIERNEY. Do you see a scenario where having the provision for a warrant somehow limits the amount of collection that could be done? I mean, can't we both have a process that allows for a warrant when it is appropriate and allows for us to get the information when and if we need—when and as we need it?

Mr. DEMPSEY. The government cannot listen to everything. It is selecting. It is collecting less than everything.

The question here is, what are the standards by which they pick and choose? And when the rights of Americans are at stake, there should be some judicial oversight of that choice.

At the end of the day, they will end up collecting however much they can process.

The question is, how is that focused, and how are those decisions made?

Mr. TIERNEY. Both of the statutes were really looking at the issue, not that you need a particularized warrant for a particular person or a particular place on that. They both sort of said in some instances maybe what you have to have is a process.

And the question really is whether in choosing—when the government is out there choosing—for all of the foreigners from whom we are going to collect information here, do we have a process that

is reasonably designed to identify and collect the communications of those whose communications may have foreign intelligence content. So that is what they are looking at. I think you said something similar to that in your written report.

So who should decide the reasonableness of that process? Shouldn't it be the courts? If it is not the courts, if we leave that to the Director of National Intelligence and to the attorney general, don't we have the fox watching the hen house?

And isn't it less likely that any executives—forget which party is in office now—are always going to be very lenient to themselves and see things as a rational way of what they are doing. Isn't that why we have judicial prior review of the process and of this situation?

Mr. DEMPSEY. I think that is right. And I think good people under pressure cut corners. Good people working under pressure make mistakes. And what we try to do in our democratic system is to create a set of checks and balances so that you don't have to ascribe any bad will or any negative motive to the DNI and to the Attorney General and to the members of the Intelligence Community, but we certainly have seen plenty of evidence of cutting corners in the past 6 years.

I think that we want to create that set of checks and balances and particularly this decision that we are talking about here of all of the communications that you collect and process, of all of the people that you are going to draw into the net, that process needs to be in some structure that has all three branches involved.

The CHAIRMAN. Thank you.

Mr. Tiahrt.

Mr. TIAHRT. Michael Brohm wrote an article that was published yesterday across the Nation in several papers. He was referring in his article—his article was titled, "Lawyering the War to Death." He references Jack Goldsmith, the Harvard law professor who wrote a book called, "The Terror Presidency." And in that, he said, never in the history of the United States had lawyers had such extraordinary influence over war policy than they did after September 11, 2001.

Mr. Goldsmith does not compliment the administration. In fact, he criticizes them in a couple of areas. He called a couple of interrogation techniques deeply flawed. But he does support the detention of unlawful combatants. He supports their confinement in Guantanamo. He supports trial by military commissions. He supports the Terrorist Surveillance Program. And he rejects the charge that the administration has disregarded the rule of law. He says, and I quote, the opposite is true. The administration has been strangled by the law. And since September 11th, this war has been lawyered to death.

He cites 1942 when FDR ordered the military commissions to try eight Nazi saboteurs who landed on our shores and were apprehended; and within 6 weeks, six of them were executed. He says FDR acted in a permissive legal culture that is barely recognizable to us today.

He says the criminalization of warfare is greatly concerned. And according to Michael Brohm, its ban on political assassinations de-

terred the Clinton administration from gunning down Osama bin Laden.

Now, this origination of lawyering of the war, he cites it back to the 1970s when FISA was written.

And he cites that, since then, even the CIA is weary of possible criminal charges, and it urges its agents to buy insurance against possible prosecution.

As we approach revising FISA, how do we avoid over lawyering the war against terrorism? How do we prevent ourselves from being bound up in legal morass and paperwork when the real job is to protect the country and keep it safe?

Now I have heard talk, and Mr. Dempsey referred to the legal structure shouldn't be centered on the protection of the targets of surveillance but more broadly to any person who might conceivably communicate with the target of surveillance.

How is it that you proposed, Mr. Dempsey, that when a FISA order is issued and surveillance is conducted and someone picks up the phone call, how do you avoid not being part of that conversation or monitoring that conversation?

Mr. DEMPSEY. I don't think what you said there was a quote from anything that I wrote. I think that the thing you were talking about "conceivably"—I don't think I said that.

Mr. TIAHRT. I believe it was in your testimony today.

Mr. DEMPSEY. Anyhow, what I am talking about here is a process that would, in fact, allow those communications to be kept and recorded.

Under the kind of blanket order or programatic order that I proposed and that appears in 3356 as well, the court would authorize a program of surveillance under procedures reasonably designed to focus on individuals overseas where there might be a foreign intelligence value in their communications.

Under that order, it is lawful and appropriate and legal to collect communications to and from the United States and to keep those communications, to use those communications in defense of the Nation.

At a certain point, though, some of those selection techniques and some of those filtering techniques may end up collecting a significant number of communications of Americans. And at that point there, the sort of center of gravity of the surveillance activity has now shifted so that it implicates significantly two people: the person overseas who has no rights, and the person in the United States who retains their rights. And then the question is, what do you do going forward from that point?

I think a process could be designed in which you are not discarding information. People talk about minimization as if it means you throw things away. I don't think the NSA ever throws much away, and I don't think they should, under my proposal, ignore valid intelligence, but at a certain point, you have to say, this is getting pretty close to home here. This is pretty much affecting an individual American, and now we need to go back and see if there is really a good reason for——

Mr. TIAHRT. What makes you think it is not done that way today?

Mr. DEMPSEY. Under the PAA, there is no process for that. There is no court order, and the standard under the PAA——

Mr. TIAHRT. You are speculating that it is not being done that way today; that when an American citizen ends up being part of an investigation, that there isn't some additional activity.

Mr. DEMPSEY. Under the PAA and under the law as it now stands, the administration would be required to obtain a court order only if they are intentionally targeting a known particular person, a U.S. person in the United States.

Mr. TIAHRT. But it is happening today.

Mr. DEMPSEY. That is all, but I think the question of intentionally targeting the person, who you are intentionally targeting——

Mr. TIAHRT. I guess my time is up.

Mr. DEMPSEY. I am happy to stay around——

Mr. TIAHRT. I believe that is already happening today. And I see no concern that you have raised in your study about additional—because when somebody is a citizen, he goes a completely different channel. There are procedures in place to go completely different channels.

Mr. DEMPSEY. I think we need to talk about this some more, and I am happy to do it with you afterwards; but as I understand it, under the PAA, not unless the government is intentionally targeting a particular——

Mr. TIAHRT. You are advocating if it is an—inadvertently picked up a conversation of a citizen in the United States in a surveillance, that there has to be some additional action even though they do not pursue it further.

Mr. DEMPSEY. Under the minimization rules, as I read them, the NSA is allowed to retain, analyze and disseminate the communication of that American and to use it for any number of intelligence purposes, to feed it into the criminal justice system, but also to use it in the intelligence system and so that information about the U.S. person—and in some cases, we want it to be used. It is not like we want to erect a new wall here.

As the President says, if al-Qa'ida is talking to somebody in the United States, we want to know about it. Absolutely.

The CHAIRMAN. Ms. Schakowsky.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

I wanted to talk about some of the specific language—I know it has been touched on, the word "concerning" and the word "acquisition."

In the letter from Mr. Wainstein, he dismisses the concerns about these, and we also heard Mr. Baker testify that there are times when the limits are pushed as far as they can go.

They are dismissed in his letter by saying, first, most of the hypotheticals we have heard are inconsistent with the plain language of the Protect America Act and the rest of the FISA statute.

So I wanted to know, one, if the language, and I am asking Mr. Dempsey and Ms. Graves, if the language is as clear as he says, and second, we commit that we will not use the statute to undertake intelligence activities that extend beyond the clear purpose of the statute.

Again, I hear what you are saying—you said, Mr. Baker, about the promise, but it also—and its impact, but it also seems like a new letter could change that.

And third, we will apply the statute in full view of congressional oversight as we intend to provide Congress with the consistent and comprehensive insight into our implementation and use this authority and what your felling is about that since we have not been able to get even the basic information about the formulation of this law.

So how much confidence should we have in these assurances?

Mr. DEMPSEY. One interesting thing to ask the administration, and to really put to the test what the PAA is all about, is to ask the administration, would it meet their needs if 105B card a program to authorize the acquisition of foreign intelligence by intentionally targeting the communications of a person reasonably believed to be "overseas"? That is what they talk about, but that is not what it says.

What is the gap between "a program of surveillance reasonably designed to collect the communications of persons believed to be overseas" versus "intelligence information concerning"?

Ms. SCHAKOWSKY. So you would suggest that language being preferable to—the one that it contains "concerning"—that it would be clearer.

Mr. DEMPSEY. Yes, I am not saying that that would be enough, but I think that certainly helps put to the test what we are talking about here. Are we targeting persons reasonably believed to be——

Ms. SCHAKOWSKY. So you are saying that it is not—the plain language isn't clear enough.

Mr. DEMPSEY. Absolutely not. We have all kinds of words here that appear nowhere else in the statute, and they are undefined.

Ms. GRAVES. I think I can answer your questions very quickly.

First of all, the language isn't clear, and I think you can see that if you compare what was announced as the Rockefeller-Reyes proposal that subsequently became the proposal of the chairman and Mr. Conyers, they refused to confine their power to electronic surveillance. They insisted upon having acquisition, not electronic surveillance, even as in 3356. They insisted on instituting "notwithstanding any other law," meaning it blows all of the other laws basically off the books, whether it is a pen register rule, whether it is ECPA on stored communication records. They insisted on it not being targeted or requiring that the orders that are involved be directed at a particular person or particular facility.

I think the language is exceedingly broad and is unacceptable. I think that the commitment not to interpret it the way the law would permit, the plain language, while nice, is not sufficient, especially in the aftermath of Mr. Yoo's memos, reinterpreting previous laws over a period at the Justice Department and certainly not in the aftermath—certainly not in the aftermath of assertions that you will have full view through congressional oversight when in fact you haven't even received the documents that you have requested.

And so I would say, notwithstanding the assertions in a letter by an assistant attorney general, the law is what matters, and the law

is what will stand in the coming years and tailoring that law to the particular problem is the responsibility of Congress.

Ms. SCHAKOWSKY. Do you think that this collection of business records of individuals could be authorized by this law?

Ms. GRAVES. I think that it is very clear the way they described "stored records" whether records are—whether records as they are transmitted or stored, whether they are electronic in form, which includes a range of records, business records, phone records.

I think it is very clear, the language is very clear on that point, that they intend to have access to them through orders issued unilaterally by the Government.

Ms. SCHAKOWSKY. Do you feel comforted by the comment in the line in Mr. Wainstein's letter that says we wish to make very clear that we will not use this provision to do so?

Ms. GRAVES. I believe the paragraph before that talks about not using it for library records or financial records. It is not actually a global disavowal of that power. In fact, the language itself, the Stored Records Communications Act, people who have litigated and worked on it know that it reaches very broadly, and I think that his declaiming library records in the aftermath of the library controversy with the PATRIOT Act is insufficient. And regardless of its assertions, it is the law that matters, not his interpretation of it.

Mr. DEMPSEY. I would be interested in his answer to the question, how did the Government under FISA deal with access to stored e-mail?

Ms. SCHAKOWSKY. I will ask that.

Mr. BAKER. How did we collect it?

Ms. SCHAKOWSKY. Did you have access to stored records under FISA? Was it interpreted in that way? Stored e-mail.

Mr. BAKER. You made a reference to the business records. There is a business records provision that allows you to obtain a variety of materials, any tangible thing, and then there is also FISA. We can conduct electronic surveillance and physical search of electronic mail. So we would do it depending upon the circumstances. You do one or the other. So you could conduct a search for certain types of stored e-mail, and you might do something that might be construed as electronic surveillance in other contexts.

As I said in my testimony, there are no forms of modern communications that we couldn't get to under the regular FISA.

Mr. DEMPSEY. I think that what that means then is that access to stored e-mail through a physical search is not electronic surveillance. Therefore, it falls under 105B. And so in addition to the physical search authority, which requires a court order, 105B authorizes acquisition to stored e-mail without a court order. That is a major change.

Mr. RIVKIN. I was just going to say that leaving aside the question of whether certain stored records can be accessed, to me, if you look at the language in its totality, particularly in subsection 3, that, and I quote, in laws obtaining the foreign intelligence information from—with the assistance of a communications service provider, custodian or other person who has access to communications, the notion that this would allow you to go search somebody's apart-

ment and pretend that the super in that building is a custodian is silly.

I am very aggressive when it comes to construing statutes both in my private sector days and my government days. But it just doesn't get there.

We are talking here—if you look at the language in subsection 2, the acquisition does not actually constitute electronic surveillance; we are talking about electronic surveillance being accomplished by or with the assistance of the very same phone companies. Not bursting into somebody's place of business. Not going and, you know, physically downloading data from somebody's hard computer drive. That is not how it is written. I don't see how it can be construed any other way.

Ms. GRAVES. I think it is important to read the rest of that sentence, which is, "access to communications either as they are transmitted or while they are stored or equipment that is being stored or maybe used to transmit or store such communications." "Such communications" are your e-mails, your phone calls, whether they are about business matters, health matters, intimate conversations with your loved ones. Those communications, that is an enormous universe of private communications of Americans.

And I don't think that saying that you are not directly going to go after a library's records is sufficient.

And also, in the aftermath of this "notwithstanding any other law" language, it is not clear how this affects the National Security Letter authorities that have been not adequately supervised. It is not clear how it affects other laws. They have carved out another opportunity to interpret it in a number of ways, and "communications" alone encompasses almost all of the things we do as we communicate to each other every day on laws or other matters.

The CHAIRMAN. Mr. Holt.

Mr. HOLT. Thank you, Mr. Chairman.

Let me first ask consent to have put in the record a letter to me from Debra Jacobs, executive director of the New Jersey Civil Liberties Union, dated August 22nd.

Let me begin with two rhetorical questions that I am not going to ask you to take time to answer.

Would you say that a characteristic of regimes that we detest and condemn around the world is that they spy on their own people? And would you say these regimes often say they are doing so to preserve the safety and security of their people?

I will let those stand as rhetorical questions.

And rather than trying to pull at pieces of what I think is a seriously flawed piece of legislation, let me go back to the beginning.

Mr. Dempsey, you say that the Director of National Intelligence laid out three basic requirements for FISA legislation or reformed FISA legislation. No particularized orders for surveillance designed to intercept the communications of foreigners overseas, a court order for surveillance of Americans and immunity for service providers.

Do you believe that FISA as it existed before reformed a month or so ago provided that there were no particularized orders required for interception of foreigners' communications?

Mr. DEMPSEY. There was no requirement for foreign-to-foreign. On foreign-to-domestic, the law had two different——

Mr. HOLT. So for foreign-to-foreign, you think it really required no change or even clarification; is that correct?

Mr. DEMPSEY. A clarification may have been helpful. There seemed to be some concern and confusion and a lot of debate about it. I always thought that a clarification was desirable.

Mr. HOLT. Would you say that it required reform or clarification for foreign-to-foreign communication, Mr. Baker?

Mr. BAKER. The difficulty it seemed to me was not saying whether—let me back up.

One of the toughest problems to deal with, I think, that you have to confront is the situations we have talked about a little bit today where you cannot tell where the communication is to or from or both. That is the hard question here.

So foreign-to-foreign——

Mr. HOLT. So that was unclear you are saying?

Mr. BAKER. No. I am saying it is clear. I thought it was clear with respect to foreign-to-foreign wire or radio communications. I think it is more difficult if you move outside those definitions.

Mr. HOLT. And what kind of language, Mr. Dempsey, what kind of language change would you suggest or would you have suggested last July to incorporate foreign-to-foreign communications that might pass through the U.S.?

Mr. DEMPSEY. Well, I think there is language in 3356 that is quite clear: A court order is not required for the acquisition of contents of any communications of persons located outside of the United States even if they pass through the U.S.

Mr. HOLT. The DNI also says there should be court orders for surveillance of Americans. Do you think FISA, as it existed before, provided that?

Mr. DEMPSEY. Yes, clearly.

Mr. HOLT. And as for immunity for service providers that cooperate with the Government, let me ask, first of all, service providers have an obligation or a responsibility to comply with illegal surveillance requests?

Mr. DEMPSEY. Yes, I think to be fair——

Mr. HOLT. I said with illegal service requests.

Mr. DEMPSEY. That they wanted to have the ability to compel them to cooperate and to have immunity for a lawful cooperation, for cooperation for lawfully authorized orders.

Ms. GRAVES. I think I heard your question correctly, and I think it is very clear under FISA. FISA was intended to prevent that scenario, prevent compliance and punish compliance with unauthorized orders for surveillance that did not involve either a court or an emergency permitted under the statute.

Mr. HOLT. What I hear you saying, and I am sorry we don't have more time to explore in depth all of these, is that the changes necessary in the FISA that we knew and some people loved and some people hated for years with all of its various revisions, needed rather minor modification to provide what the Director of National Intelligence said was needed.

Now, let me explore a couple of other points.

Do you think, Mr. Dempsey, that it is important that any such legislation be identified as the exclusive means?

Mr. DEMPSEY. I think it is critical. It is a critical element.

Ms. GRAVES. If I could interject.

I think that making the PAA exclusive would be really not useful because it creates such enormous exceptions. Reinforcing the exclusivity of FISA I am ambivalent about because I think it is extremely clear that it is the "exclusive means", and it should have been clear for any lawyer at the Justice Department that it was the exclusive means.

Mr. HOLT. So many questions so little time.

Let me ask, of course, what really concerns me is that, administratively, it is so easy to fall into the pursuit of enemies list or chasing hobgoblins with the best of intentions and with the most patriotic intentions even and without judicial review of determination of probable cause. I am really concerned about that. Who determines who is the bad guy?

But my question is, does after-the-fact minimization take the place of judicial review? And let me ask Ms. Graves and Mr. Dempsey that.

Ms. GRAVES. I would say that I don't think it is adequate, and I think, as Mr. Dempsey wrote in his testimony, the courts, while there has been some discussion of what the courts did hold, one of the things they did hold was that minimization itself was not sufficient; and they also held, with respect to Americans, you needed to have some individualized determination even if there was some leeway before Congress passed FISA to do so without a warrant.

And I would say that the minimization procedures are certainly not adequate. If we are talking about expanding the reach of the NSA into the global communication network in the United States, it is utterly inadequate to attach minimization to the PAA.

Mr. DEMPSEY. I will stand on what the Supreme Court said in Katz in 1967. There the police did everything right. They fully minimized, they had probable cause, and the court still said that was an unconstitutional search because these decisions are not to be made solely by the executive branch.

Mr. HOLT. And that decision has not been nibbled away at over the course of years.

Mr. DEMPSEY. Not that one.

The CHAIRMAN. Ms. Wilson.

Mrs. WILSON. Mr. Baker, I had a couple of questions for clarification, if you would.

When did you leave the Justice Department? In which year?

Mr. BAKER. I am currently on leave from the Department. I have been on leave from the Department since January of this year. I am on leave without pay. I am sitting here uncompensated.

Mrs. WILSON. So you have not been involved in the year 2006 in matters relating to the FISA court?

Mr. DEMPSEY. 2006 I was.

Mrs. WILSON. January 2007.

So you were not aware of the problems that have occurred in 2007 with respect to timeliness of warrants?

Mr. BAKER. I am aware of the issues that have arisen in 2007 because I have regular contact with folks at the Department.

Mrs. WILSON. Would you characterize those in unclassified session?

Mr. BAKER. I don't believe I can.

Mrs. WILSON. But you are aware that problems exist this year that did not exist before?

Mr. BAKER. I am aware of what happened in January, and I am aware of what happened subsequently, the event that lead up to the Protect America Act. I am not there every day, obviously, but I have had discussion with folks there.

Mrs. WILSON. In some of your answers to previous questions, you talked about the timeliness in terms of emergency warrants and the reputation of your office as being the rusty gate and so forth.

You responded that you do those as quick as you possibly can. And it can happen extremely quickly to get an emergency warrant.

Have you ever been involved in an emergency warrant or an emergency application for a warrant that has taken more than an hour?

Mr. BAKER. Yes.

Mrs. WILSON. More than 6 hours?

Mr. BAKER. I guess the question is, what do you mean it has taken more than 6 hours? From the time—what I assess that means is from the time that the intelligence agency——

Mrs. WILSON. From the time that the intelligence agency says, we have got a number, we need to get up on it, to the time they can turn on the switch, has it taken more than an hour?

Mr. BAKER. I can't answer that because all I can control is the time——

Mrs. WILSON. From the time you were first informed that one would be required to when it was—to when they were able to turn on the switch, were there any that took longer than 6 hours?

Mr. BAKER. I am not trying to be cagey. We did lots of these things. We did them all the time. We tried not to over-lawyer the situation so we delegated authorities to folks within our organization to take prompt action on these things.

Did some take more than 6 hours? Certainly possible. I don't know. We didn't keep track. We didn't keep statistics on that.

But what I am reporting to you, I believe, is that, overall, my assessment is that the system was successful. Could the system have done more with more resources? Of course. Could the system have done more if you didn't involve all of these lawyers in it? Yes. I mean——

Mrs. WILSON. I am actually asking a more specific question which I think is a legitimate one.

In your experience, your direct personal experience, did you ever have a case where it was more than 6 hours between the time you first became aware a warrant, an emergency warrant would be needed to when it was signed off on?

Mr. BAKER. Yes, in that particular question.

Mrs. WILSON. How about 12 hours?

Mr. BAKER. I don't remember.

Mrs. WILSON. My point here is that time matters. If it was in a domestic circumstance—for example, we have Amber Alerts all the time in my community. If it was your kid whose life was at stake, is 6 hours fast enough?

Mr. BAKER. That is—6 hours is obviously not fast enough in that situation. But the question is——

Mrs. WILSON. Imagine a circumstance where it is a FISA warrant that is needed where 6 hours isn't fast enough.

Mr. BAKER. You are making the judgements about how you want the law constructed. I am trying to give you the benefit of my experience so that you can make an informed judgment. It is up to you to decide what the law is going to be. Having said that, we worked long and hard to make sure we gave the Intelligence Community what it needed when it needed it.

Mrs. WILSON. Do you understand why there might be frustration?

Mr. BAKER. I understand completely. I have heard it—you know, when you have lawyers involved in between the intelligence operatives and the thing that they want, there is going to be tension; there are going to be difficulties.

My job was to enforce the law that this Congress—not this Congress but that Congress had enacted, and that is what I did in my level best to achieve.

Mrs. WILSON. Let me ask you, Mr. Dempsey, about a Supreme Court decision in 1990, United States v. Verdugo. In that case, Justice Rehnquist said that, "At the time of the search, this particular individual was a citizen and resident of Mexico with no voluntary attachment to the United States, and the place searched was located in Mexico. Under these circumstances, the Fourth Amendment has no application.

He further said that, "The result of accepting this Mexican individual's claim would have significant and deleterious consequences for the United States in conducting activities beyond its borders. The rule would apply not only to law enforcement operations abroad but also to other foreign policy operations which might result in searches or seizures. Application of the Fourth Amendment to those circumstances could significantly disrupt the ability of the political branches to respond to foreign situations involving our national interests."

And in that case, they determined that the Fourth Amendment, that this gentleman had no Fourth Amendment protections.

Are you familiar with that case?

Mr. DEMPSEY. Yes, I am. There was no American involved in that case.

Mrs. WILSON. Do you believe that warrants should be required for foreigners in foreign countries when we are targeting that person?

Mr. DEMPSEY. No. Absolutely not.

Mrs. WILSON. If that Mexican were talking to an American, would a warrant have been required?

Mr. DEMPSEY. Then you have got two people on the conversation and you have got rights on the American side.

Mrs. WILSON. Would a warrant have been required?

Mr. DEMPSEY. I think if that is an ongoing surveillance that is collecting information about the American, yes.

Mrs. WILSON. They were targeting a Mexican in Mexico.

Would a warrant have been required?

Mr. DEMPSEY. As I said, I don't think that the targeting question is the relevant question here.

Two people's interests are at stake. In the Verdugo case, only one person's interest were at stake: a Mexican national in Mexico. He had no rights under the Constitution. When you switch to foreign-to-domestic, and you are talking about two parties, we have to look at both sides of the equation.

Mrs. WILSON. If a Mafia Don is under electronic surveillance in this country and he talks to his son's teacher, is a warrant required for his son's teacher?

Mr. DEMPSEY. A warrant is required to intercept those communications. Not on the teacher.

Mrs. WILSON. Does the son's teacher have any rights——

Mr. DEMPSEY. Absolutely.

Mrs. WILSON. That their rights under the constitution have been violated?

Mr. DEMPSEY. Well, her rights haven't been violated because there is a court order. On the other hand, if there was no court order and the teacher's conversations were intercepted, that teacher has a constitutional violation, and the Government could not use that information against the teacher.

When the judge issues the order against the Mafia Don, the judge is saying there is probable cause to believe that the Mafia Don is a criminal and there is probable cause to believe that the communications facilities that are going to be the target of the surveillance are being used.

The CHAIRMAN. Can you wrap it up because we have to leave.

Mrs. WILSON. If we are lawfully listening to someone overseas for a foreign intelligence purpose, how can you tell who they are going to call before they call?

Mr. DEMPSEY. You can't in advance——

Mrs. WILSON. Which means we need a warrant for every conversation.

Mr. DEMPSEY. No, Congresswoman. Nobody has argued that. Nobody has said that the Government needs to know in advance what the person overseas is doing. The whole purpose of the program warrant is to allow the Government to be begin monitoring, not knowing who the target overseas——

Mr. RIVKIN. What Mr. Dempsey, with all due respect, is suggesting, if an individual overseas is communicating enough with the United States, in order to continue monitoring that individual's communication, you need to get a warrant against him because you surely cannot get a warrant against an innocent American he is communicating with.

Ms. GRAVES. I would disagree. That interpretation is not an accurate characterization of what we have suggested, and, in fact, if you look back at the original Rockefeller-Reyes proposal, there was a very sensible approach to the circumstance in which an American—you learn subsequently that an American's communications are involved or there are significant communications or significant number of communications with an American. Our understanding is that the administration tried to deflect that approach by suggesting that if foreigners call the American Airlines, we will have to get a warrant for American Airlines. That, I think, is an absurd

interpretation of that language, and we think that it is important to protect the interest of Americans, and we think the Americans in your district and other districts do require that protection.

Mrs. WILSON. I would agree that we need to protect the civil rights and liberties of Americans. We also need to be able to protect this country from terrorists communicating overseas. And I hope that in future public discussions and public testimony, we will have panels who are much more familiar with how these operations take place.

Thank you, Mr. Chairman.

The CHAIRMAN. And with that, let me finish up because we have to relinquish the room. I want to thank all of the panelists for their expertise and testimony here. As you can see, there are issues that we have to work out, but we must work them out because it is in our best interest to protect our national security.

Thank you very much. The hearing is adjourned.

[Whereupon, at 1:25 p.m., the committee was adjourned.]

○