S. HRG. 110–921

STRENGTHENING FISA: DOES THE PROTECT AMERICA ACT PROTECT AMERICANS' CIVIL LIBERTIES AND ENHANCE SECURITY?

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

SEPTEMBER 25, 2007

Serial No. J–110–57

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

53–358 PDF WASHINGTON : 2009

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

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00001 Fmt 5011 Sfmt 5011 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
BENJAMIN L. CARDIN, Maryland
SHELDON WHITEHOUSE, Rhode Island

ARLEN SPECTER, Pennsylvania
ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
JON KYL, Arizona
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina
JOHN CORNYN, Texas
SAM BROWNBACK, Kansas
TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
MICHAEL O'NEILL, *Republican Chief Counsel and Staff Director*

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00002 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

Page

Feingold, Hon. Russell D., a U.S. Senator from the State of Wisconsin, prepared statement 186
Grassley, Hon. Chuck, a U.S. Senator from the State of Iowa, prepared statement 188
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont 1
prepared statement 190
Specter, Hon. Arlen, a U.S. Senator from the State of Pennsylvania 3

WITNESSES

Baker, James A., Lecturer on Law, Harvard Law School, Formerly Counsel for Intelligence Policy Department of Justice, Washington, D.C. 46
Cunningham, Bryan, Principal, Morgan & Cunningham, LLC, Greenwood Village, Colorado 51
Dempsey, James X., Policy Director, Center for Democracy and Technology, San Francisco, California 49
McConnell, J. Michael, Director, Office of the National Intelligence, Washington, D.C. 6
Spaulding, Suzanne E., Principal, Bingham Consulting Group, Washington, D.C. 53

QUESTIONS AND ANSWERS

Responses of James A. Baker to questions submitted by Senators Specter, Leahy, and Kennedy 64
Responses of Bryan Cunningham to questions submitted by Senators Specter and Leahy 83
Responses of James X. Dempsey to questions submitted by Senators Leahy, Specter and Kennedy 107
Responses of J. Michael McConnell to questions submitted by Senator Specter (**Note:** Answers to Senators Durbin, Feingold, Kennedy and Schumer were not received at the time of printing, November 3, 2009) 119
Responses of Suzanne Spaulding to questions submitted by Senator Kennedy . 140

SUBMISSIONS FOR THE RECORD

Baker, James A., Lecturer on Law, Harvard Law School, Formerly Counsel for Intelligence Policy Department of Justice, Washington, D.C., statement . 149
Cunningham, Bryan, Principal, Morgan & Cunningham, LLC, Greenwood Village, Colorado, statement 156
Dempsey, James X., Policy Director, Center for Democracy and Technology, San Francisco, California, statement 168
McConnell, J. Michael, Director, Office of the National Intelligence, Washington, D.C., statement 192
Spaulding, Suzanne E., Principal, Bingham Consulting Group, Washington, D.C., statement 211
Sussmann, Michael A., Partner, Perkins Coie LLP, Washington, D.C., statement 225

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00003 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

STRENGTHENING FISA: DOES THE PROTECT AMERICA ACT PROTECT AMERICANS' CIVIL LIBERTIES AND ENHANCE SECURITY?

TUESDAY, SEPTEMBER 25, 2007

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Committee met, pursuant to notice, at 9:33 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Kennedy, Feinstein, Feingold, Durbin, Cardin, Whitehouse, Specter, Hatch, Kyl, Sessions, and Coburn.

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

Chairman LEAHY. Good morning. Before we start, just so everybody will understand, there seems to be, certainly more than I am used to, people having demonstrations in hearings. Now, just so everybody understands, I want everybody to be able to watch this hearing. I want everybody to be able to watch it comfortably. If people stand up and block the view of others who are here, they will be removed.

If there are any demonstrations, whether they are for or against a position I might take, for or against a position Senator Specter might take, for or against a position anybody else or the witness might take, for or against it, they will be removed. I am sure that is not going to be necessary. I am sure everybody is going to treat this with the decorum expected. But if somebody is tempted otherwise, the police will be instructed to remove you.

Now, this Committee holds this hearing today to consider the Protect America Act that was passed in haste in early August.

Congressional leaders went to extraordinary lengths earlier this summer to provide the flexibility Director McConnell said was needed to fix a legal problem with surveillance of targets overseas. I supported a change to FISA, as I have done several times since 9/11. In fact, I think I have supported some 30 changes to FISA since it was written.

The Rockefeller-Levin legislative proposal that many of us voted for would have eliminated the need to get individual probable cause determinations for surveillance of overseas targets. That bill addressed the concerns that had been raised by an opinion of the FISA Court, and it satisfied what the administration said was needed in that time of heightened concern. Yet Director McConnell

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00005 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

and the administration rejected that legislation, and we need to find out why.

I do not know who Director McConnell is referring to in his written testimony when he says that he has "heard a number of individuals . . . assert that there really was no substantial threat to our Nation." I trust that he is not referring to any Senator serving on this Committee, but if he did, I hope he would feel free to say so.

Let me be clear: I have talked to virtually every Senator in this body. Every single Senator understands the grave threats to our Nation. Every single Senator, Republican or Democratic or Independent, wants us to be able to conduct surveillance effectively. Every Senator on this Committee voted to give Director McConnell the flexibility he said he needed. So I hope we will not hear any more irresponsible rhetoric about congressional inquiries risking Americans' safety. We all want Americans to be safe. Our job is to protect Americans' security and Americans' rights. We also take an oath of office, every one of us.

The Protect America Act provides sweeping new powers to the Government to engage in surveillance, without a warrant, of international calls to and from the United States and potentially much more. It does this, in the view of many, without providing any meaningful check or protection for the privacy and civil liberties of the Americans who are on these calls. We are asked to trust that the Government will not misuse its authority. When the issue is giving significant new powers to Government, "Just trust us" is not quite enough.

Fortunately, those temporary provisions contain a sunset. We meet today to consider real issues and concerns with this legislation. Let us not engage in the high-pitched rhetoric that plays on people's fears, because that prevents real progress.

The FISA Court has played an important role ever since the Foreign Intelligence Surveillance Act was passed. It provides a meaningful check on the actions of our Government as it is engaged in surveillance of Americans. Unfortunately, the FISA Court was cut out of any meaningful role in overseeing surveillance of Americans in the Protect America Act.

The Rockefeller-Levin measure by contrast would have allowed the "basket" surveillance orders that the administration says are needed, and Director McConnell says are needed, with no individual probable cause determinations, but it at least had the FISA Court issuing those orders to communications carriers after reviewing the administration's procedures. The Protect America Act, the one that was passed, requires U.S. telecommunications carriers to assist with surveillance just on the say-so of the Attorney General and the Director of National Intelligence. That is a mistake; it is an invitation to abuse.

So I look forward to hearing from Director McConnell on what he believes the problems are with a role for the FISA Court in issuing orders, and how we can create the necessary authority to include the appropriate checks and balances.

The problem facing our intelligence agencies is targeting communications overseas. We want them to be able to intercept calls between two people overseas with a minimum of difficulty. What

changes the equation and raises the stakes is that the people may be innocent Americans, or they may be talking to innocent people here in the United States. International communications include those of business people or tourists; they even include the families of our troops that are overseas. Now, we can give the Government the flexibility it needs to conduct surveillance of foreign targets, but we can do it while doing a better job protecting the privacy of individual Americans.

The Protect America Act provides no meaningful check by the FISA Court, or by the Congress, for that matter. It does not even require the Government to have its own internal procedures for protecting the privacy of these Americans. As I said, it may be a spouse calling from here to a husband or a wife who is overseas protecting America. They may be talking about the children's grades. They may be talking about a difficulty a child may be having with the separation. Now, the alternative bill would have required at least internal procedures and an Inspector General audit, and I would like to know why Director McConnell rejected that idea.

In addition, the Protect America Act contains language that appears to go far beyond what the administration said it needed. It redefines "electronic surveillance" in a way that has expansive implications, but was not necessary to accomplish the administration's stated objectives. It has language in many places that, at the very least, is inscrutable and could be read to allow much broader surveillance than the administration has acknowledged or, for that matter, I hope intends. And if this was unintentional, well, then, we can fix it. That is one of the things the sunset requires us to do, is look at it. If it was not, then we need to evaluate what was really intended and why.

I know the skilled and dedicated employees of our intelligence agencies want to protect our country, as every one of us does. But if our history has taught us anything, it is that the Government cannot and should not be left to police itself when it comes to the secret surveillance of Americans. The Founders knew it. The Congress that passed the Foreign Intelligence Surveillance Act knew it. So I hope this hearing will help us institute the proper protections to safeguard our security and our valued freedoms.

As I said, we have amended FISA about 30 different times since it was enacted. Many of us have served here long enough on this Committee to have voted for every one of those changes.

Senator Specter.

STATEMENT OF HON. ARLEN SPECTER, A U.S. SENATOR FROM THE STATE OF PENNSYLVANIA

Senator SPECTER. Thank you, Mr. Chairman.

The Congress will soon be called upon to decide what to do on the application by the administration to have wiretapping surveillance overseas without warrants. We passed legislation in early August, at 11:59 at the last minute, relying really, Mr. Director, on your advice that there were dire threats to the United States at that time.

And the congressional response to the administration's request really depends largely on trust, and the sequence of these

warrantless wiretaps has strained that trust relationship because the administration put into effect a program for warrantless wiretaps different from the tradition of applying to a judge, showing probable cause to get judicial authorization for a wiretap, not disclosed to Congress until the newspapers broke the story in December of 2005, when we were in the middle of the final stages of debate on the PATRIOT Act.

It delayed the passage of the PATRIOT Act, almost scuttled the PATRIOT Act. And my response at that time was that the administration could at least have confided in the Chairman of the Judiciary Committee and the Ranking Member—I was then Chair, Senator Leahy ranking—and similar ranking Chairs on other key Committees. But the administration chose not to do so, and that kind of a policy I think needs to be revisited.

Then when you came forward, Mr. Director, in late July and advised the Congress about the threats which you posed, the chatter which was being undertaken, it was in reliance on your representations that the legislation was enacted. And it is really vital that we not wait until the last minute to make another hasty decision.

We carefully sunsetted the provisions for warrantless wiretaps directed at people overseas for a 6-month period of time. When you talk about some public disclosure or some public understanding of threats to the Nation, it is obvious we are in a very difficult situation because you cannot—you are the Director of National Intelligence. You cannot say too much. And perhaps much of it has to be transmitted to the key committees in a closed session.

But the business of warrantless wiretaps is a matter of enormous public concern, and I believe there has to be more consideration given to what can be disclosed publicly, as transparently as possible so the American people know what the intrusion is, they know what the reasons are, and we can undertake a balancing test to see if it is warranted. That is what I think we have to do. So to the extent you are talking about threats, to the maximum extent they can be disclosed consistent with national security, I think that is advisable.

When we talk about targeting overseas and targeting foreigners overseas, there is a significant difference between targeting people in the United States for wiretaps. And I am glad to see the administration finally brought the issue for targeting Americans in the United States to the FISA Court. We struggled with many hearings in the 109th Congress and finally came to that conclusion.

When you are targeting overseas, I think there has to be a sharp distinction between targeting U.S. citizens overseas and targeting others. Right now there is an Executive order which requires the Attorney General to find probable cause before a U.S. person is targeted overseas. And my thinking is that the statute ought to be modified to put that responsibility in the FISA Court, to establish probable cause, which is the equivalent of authority to issue a warrant, if targeting is being directed at U.S. persons.

The administration has argued that the FISA Court ought to be limited just as to procedures, that the administration requires that flexibility. I believe we need more of a showing by you, Mr. Director, of the need for that flexibility, and the elimination of the su-

pervision of the FISA Court has to be justified by real necessity for your flexibility.

And I believe it is not sufficient for the FISA Court to be taking a look at procedures every year. I am not sure how often it ought to be. Perhaps every few months. But I think when the renewal is made to the FISA Court, even as to procedures, there ought to be a showing as to what you have accomplished. This invasion of privacy, no matter whose privacy is involved, has produced some results. So we are going to be weighing these factors very carefully.

One final comment. There has been discussion as to the participation of your counsel in this matter. You called me. I know you have discussed it with a number of members of the Committee, and Senator Leahy and I have discussed it. And if you have a legal issue and need the advice of counsel, my judgment would be that you ought to have significant latitude. You are not a lawyer. If you need an interjection by legal counsel, I think you ought to be able to do that, too. But we will have to make those judgments as the specific questions arise.

You have some lawyers on the panel, including the Chairman, myself, Senator Hatch, Senator Kennedy, Senator Feinstein—smarter than most of the lawyers on legal issues because of her heavy study of the matter. She cites more sections of more codes than anybody else on the Committee. And the Senator from Maryland is also an attorney, so we will be watching very closely to make sure that you have an adequate opportunity to respond or get assistance on the very complex legal issues which are involved here.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you. And as I told Senator Specter earlier this morning when we discussed this, I have written to Director McConnell and thanked him for his offer of having Government witnesses and lawyers here to testify, too. Of course, they have not submitted testimony, and so I declined. We are dealing with more with factual issues than legal issues. We will be going through those, among others, at the time of the Attorney General nomination hearing.

I also explained to Senator Specter—and I should explain to you, Admiral—that should you have a legal question and you wish to consult, we have several of the best lawyers in the city behind you. Should you wish to consult, feel free to do so. That time that you take to do that will not come out of either your time or the Senator's time asking you the question. Just so you know that.

Of course, also, as I have explained for years and years on various committees I have chaired, I do not play "gotcha." The record will stay open for a certain period of time to allow you a chance to look through it and make any corrections you wish.

Senator HATCH. Mr. Chairman.

Mr. Chairman, if there are technical legal questions, I think the Director is not an attorney and he ought to be able to call on his people to be able to help us with those direct legal questions. So I just—

Chairman LEAHY. Well, we will have plenty of time for them to do that, and should the administration want them to come up and testify on the legal thing, we will try to find a time so they can do

just that, in the normal forum with their testimony provided to you and me and everybody else on the Committee ahead of time.

Senator HATCH. My only point, Mr. Chairman, is that some of us would benefit from perhaps some legal answers from Government officials, because we will get some from other witnesses, and we ought to at least be able to judge that.

Chairman LEAHY. If the administration wishes to have them come up and be sworn and testify, we can probably arrange that.

Senator HATCH. Thank you, Mr. Chairman.

Chairman LEAHY. Please stand and raise your right hand. Do you solemnly swear that the testimony you will give in this matter will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. MCCONNELL. I do.

Chairman LEAHY. Thank you. Director McConnell, we have your full statement, and, of course, it will be made part of the record so that we can get into questions. Would you please summarize it as you see fit and we can get into questions.

STATEMENT OF J. MICHAEL MCCONNELL, DIRECTOR OF NATIONAL INTELLIGENCE, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, WASHINGTON, D.C.

Mr. MCCONNELL. Thank you, Chairman Leahy, Ranking Member Specter, and other members of the Committee. Thank you for inviting me to appear here today. I appreciate the opportunity to discuss the 2007 Protect America Act and the need for lasting modernization of the Foreign Intelligence Surveillance Act that we will refer to in the hearing, I am sure, as "FISA."

Before I begin, I need to note that some of the specifics that support my testimony cannot be discussed in open session. I understand, and I am sensitive to the fact, that FISA and the Protect America Act and the types of activities that these laws govern are of significant interest to Congress and to the public.

And for that reason, I will be as open as possible, but much of this discussion comes with some degree of risk. This is because open discussion of specific foreign intelligence collection capabilities causes us to lose those very same capabilities. Therefore, on certain specific issues, I would be happy to discuss with members in a classified setting.

I have previously appeared before the Intelligence Committee in closed sessions, which includes crossover members for this Committee. I would be happy to appear before this Committee in closed session as well so that you may avail yourselves of any additional information that would be helpful in considering these very important issues.

Chairman LEAHY. If there are things that we should be doing in closed session, I will confer with Senator Specter, and I am sure he and I can arrange such a closed session.

Mr. MCCONNELL. Thank you, sir.

It is my belief that the first responsibility of intelligence is to achieve understanding and to provide warning. As the head of the intelligence community, it is not only my desire, it is my duty to encourage changes to policies and procedures, and where needed, legislation, to improve our ability to provide warning of terrorist or

other threats to the country. On taking up this post, it became clear to me that our foreign intelligence collection capabilities were being degraded.

I had learned that collection using the authorities provided by FISA continued to be not only instrumental but vital in protecting the Nation. However, due to changes in technology, the wording of the law as it was passed in 1978 was actually preventing us from collecting foreign intelligence information.

I asked what we could do to correct the problem, and I learned that a number of my colleagues had already been working on the issue. In fact, in July of 2006, the Director of the NSA, General Keith Alexander, and the Director of CIA, General Mike Hayden, testified before this Committee regarding proposals to change and update FISA. That 2006 testimony contained significant information and insight into our capabilities and the need for changes to wording in the law.

I also learned that Members of Congress in both chambers and both sides of the aisle, to include this Committee, had proposed legislation to modernize FISA in 2006. A bill passed the House last year, but it was not taken up by the Senate. Therefore, the dialog on FISA has been ongoing for some time. It has been a constructive dialog, and I hope it continues in furtherance of serving the Nation to protect our citizens, both their safety and their civil liberties. None of us wants a repeat of the 9/11 attacks, even though al Qaeda has stated their intention to conduct such attacks.

As is well known to this Committee, FISA is the Nation's statute for conducting electronic surveillance and physical search for foreign intelligence purposes. When passed in 1978, FISA was carefully crafted to balance the Nation's need to collect foreign intelligence information with the need for the protection of civil liberties and privacy rights of our citizens. There were abuses of civil liberties from the 1940's through the 1970's that were galvanized by the abuses of Watergate that led to the action that caused the Congress to craft and pass the legislation that was signed by President Carter in 1978.

This 1978 law created a special court, the Foreign Intelligence Surveillance Court, to provide judicial review of the process. The Court's 11 members devote a considerable amount of time and effort to FISA matters, while at the same time fulfilling their district court responsibilities, and we are indeed grateful for their service.

FISA is a very complex statute. It has a number of substantial requirements. Detailed applications contain extensive and factual information and require approval by several high-ranking officials in the executive branch before going to the court. The applications are carefully prepared, subject to multiple layers of review for legal and factual sufficiency to ensure that they meet the probable cause standard to the Court.

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

Why did we need the changes that the Congress passed this past August? FISA's definition of "electronic surveillance" simply did not keep pace with technology and therein is the issue. The definition

of "electronic surveillance" from the 1978 law did not keep pace with technology. Let me explain what I mean.

FISA was enacted before cell phones, before e-mail, and before the Internet. The Internet was not even envisioned in 1978. Today it is a tool used by hundreds of millions of people, to include terrorists for planning, training, and coordination of their operations.

When the law was passed in 1978, almost all calls were on a wire in the United States, and almost all international calls were in the air, or known as "wireless" communications. Therefore, FISA was written in 1978 to distinguish between collection on a wire and collection out of the air.

Today the situation is completely reversed. Most international communications are on a wire, fiber optics, and local calls are in the air. FISA originally placed a premium on the location of the collection, and that is a very important issue for us to consider. Therefore, collection against a foreign target located overseas, because of the wording in the law, from a wire located in the United States, required us to have probable cause standards to seek a warrant from the FISA Court to collect against terrorists located overseas.

Chairman LEAHY. But, Director, you have emphasized over and over again the 1978 law. It has been amended about 30 times since then, around 7 or 8 times at the request of the administration with which you serve. And I think it is somewhat disingenuous to keep referring to the fact that we were dealing with a 1978 law. It has been dramatically changed since that time.

Now, you have testified a number of times over the past few weeks. I know that it is difficult. We all appreciate the time you have taken. But just as I have concerns with you talking as though we are dealing with a 1978 law, I have concerns about some of the statements you made in those hearings.

For example, 2 weeks ago in Senate testimony, you claimed that information obtained as a result of the Protect America Act, the latest change in the FISA Act, was important to the investigation of the recent German terror plot. You said it several times. But later, after press reports and Members of Congress questioning it, you issued a statement saying your testimony was not true. The information you spoke of was obtained before the latest law was enacted. It was obtained under the old FISA authority.

In the same hearing, you warned that if we would lose the authority in the new legislation, you would lose 50 percent of our ability to track, understand, and know about these terrorists. A week later, when you testified before the House Judiciary Committee, that 50 percent had moved to two-thirds of our capability. And in that same hearing, you said you were concerned that losing the authority would shut us down. So you went from 50 percent to 100 percent in no time whatsoever.

Now, I am just wondering why did you testify to something that was false and give a misleading impression of the benefits of the legislation. Did you check with anyone before making those claims?

Mr. MCCONNELL. Sir, when I was asked about FISA and the situation in Germany, the question that I understood was referring to FISA. This panel is making a differentiation between FISA and the Protect America Act. In my mind, that is all one act passed in

1978, as you have mentioned several times, updated any number of times. In my view, it was updated in August as the latest review.

So the question I understood was did FISA make a difference, and FISA was absolutely vital for us to understand that threat and to assist in what happened in terms of removing terrorists whose intent was to kill Americans and/or Germans in Germany.

Chairman LEAHY. And I appreciate your explanation of what did appear to be misleading to most people. But, you know, if a well-intentioned person like can make such mistakes, you can understand why we need to have some checks on this so that mistakes are not made.

We all believe that conducting surveillance on terrorism is vital. I voted to give you greater flexibility, as did everybody on this Committee, when that matter came before us in early August. Some of us did not vote for the Protect America Act, but we voted for the Rockefeller-Levin amendment, the alternative. It would have given the same flexibility, but it would have had some oversight by the Court and more requirements for the executive branch to protect privacy.

When you testified in the past few weeks-and it sounded like you were saying that here—you always warned about the dangers of going back to the old FISA process with individual probable cause determinations. Well, let us be honest. Neither the Rockefeller-Levin bill nor the similar House alterative would have required that. I discussed this with you many times. I said I am not asking for that. Nobody was asking for that.

So I do not know why we keep hearing about legislation that few, if any, members have proposed or supported. I would like to keep our focus on the Protect America Act and those parts that concern this Committee.

So assume that we do not propose going back to individual probable cause determinations by the FISA Court, as you seem to imply, and nobody—certainly I have never heard it from any Senator for overseas targets and not U.S. persons. If we are not going to back to individual probable cause determinations, wouldn't that help you?

Mr. MCCONNELL. That is exactly the point, Senator. Not having to be required to do probable cause justification to conduct surveillance against the known terrorist overseas is the whole point. That—

Chairman LEAHY. But nobody has suggested that. We talk about programmatic; even with the emergency time, you have after-the-fact determination. What I worry about when I hear you testify, when I hear the President give his Saturday morning speech, you always talk about this 1978 bill. I mean, that is like saying that if you go out with your brand new car and say, Boy, I remember the problems I had in my 1978 car. It is not the same one. It may be the same make of car, but it is a big difference.

Mr. MCCONNELL. Senator, all I can respond is to say I wish some of those 30 changes that you are mentioning had, in fact, addressed this issue. Now, this is not a new issue to this Committee.

Chairman LEAHY. But the Rockefeller-Levin did not require individual probable cause.

Senator HATCH. Mr. Chairman, can we let him finish his statement? I mean, I would really like to hear—

Chairman LEAHY. Would you let the Chairman finish his question, please?

Senator HATCH. Well, I thought we were going to let him finish his statement.

Chairman LEAHY. We will give you plenty of time to—

Senator HATCH. Well, let the man finish his statement.

Chairman LEAHY.—give the administration's position, but the Rockefeller-Levin did not require that individual probable cause, did it?

Mr. MCCONNELL. Sir, the issue with the Rockefeller—Levin bill is—as I tried to highlight in my statement, this is an extremely, extremely complex bill. The issue was we exchanged between us, between the Hill and the administration, seven different drafts. I was provided a copy of that draft after debate had started on the floor of the Senate. Now, when I had a few minutes to look at the draft, what I looked to see was did it introduce things that would cause a limitation on the flexibility and effectiveness of this community to protect the country. And it did.

The specific question you are asking about, quite frankly I have not found a member on the Hill that disagrees with what you are saying. I agree with it. You agree with it. The issue is we have to get it in legislation in a way that allows us to carry out our mission.

Now, what happened in that bill, the draft of that bill, introduced uncertainty. It also addressed minimization and it addressed the issue called "reverse targeting." And when you examine the full intent of that wording, what happens is it puts us in an untenable position of not having the flexibility that we need.

Chairman LEAHY. You know, it is interesting. I was in many of those meetings with you and the White House when we talked about it, when we talked about what we were going to do. None of the concerns that you are talking about now were raised at that time. They were suddenly raised when it was on the floor, and that is when it creates the concern.

Part of that we will have to go into classified session to talk about, but you can understand why people worry about this. We have a respected lawyer in Vermont, Robert Ginsburg. He and I served as prosecutors at the same time. He is representing a client being held in Guantanamo Bay. He is worried that his calls regarding his client are being monitored by the Government. He makes calls overseas, including to Afghanistan, on behalf of his client.

Now, I am not going to ask you whether his telephone is being tapped because I would not expect you to answer that. But you can see why people worry, and I think whether it was Mr. Ginsburg, whom I happen to know, or anybody else, they would feel considerably more confident if they thought that the FISA Court at least had some oversight here.

My time is up, and I will yield to—but you and I should probably discuss that matter in a classified—

Mr. MCCONNELL. Sir, if I could respond, let me go back to our discussion. You and I had a one-on-one in a classified context. As I recall, it went for about an hour and a half.

Chairman LEAHY. And I am trying to avoid going into the specifics of what we did.

Mr. MCCONNELL. And I do not intend to go there, but I need to make three points for this Committee so that everybody understands.

When I entered back into active duty service and looked at this issue, it appeared to me we had to make some fundamental changes. Now, all the changes to FISA previously notwithstanding, the three points I tried to make—and I gathered the lawyers around me to say I do not know exactly the wording how we do this, but here are the three points:

We are disadvantaged because we are currently being required to have a warrant against a foreign target located overseas and it inhibits our capability to do our job. So we have got to fix that, whatever the proper wording is.

The second is we have to have a way to compel the private sector to assist us and to provide a reasonable level of liability protection for them.

So first point, no warrant against a foreign terrorist overseas. Compel the private sector to help us.

And the third point—and this is very important. It is very important to me; it is very important to members of this Committee. We should be required—we should be required in all cases to have a warrant anytime there is surveillance of a U.S. person located in the United States. I think that was the intent of the 1978 law. That is what was included in the Protect America Act passed in August. That is where we need to be, and anything else we do to that, we have to examine what the words mean to our effectiveness. And so that is where we are with regard to examining this law.

So my point to the administration and the Congress is we need those three points, and we need to have them passed in a way that is effective for us to carry out our mission.

Chairman LEAHY. Well, I might say parenthetically, as one who has been right into this program, I am picking my words very carefully, but when you talk about the question of immunity, you have got a warrant on actions that are going on, that pretty well immunizes anybody. I mean, if in a previous incarnation, Senator Specter and I got a search warrant to search somebody's safe deposit box, and the bank opens it up for us, the bank is immunized because they have the warrant.

I yield to Senator Specter.

Senator SPECTER. Director McConnell, picking up on those three points—

Senator SESSIONS. Mr. Chairman, just briefly, did the witness ever finish his statement? I do not know if he got to finish his statement. I know you interrupted him. You had something you were concerned about. But—

Chairman LEAHY. Well, he was—

Senator SESSIONS.—I do not think he got to finish.

Chairman LEAHY. Well, he was at that time several minutes over, and I was trying to give him—

Senator SESSIONS. His light was green. I noticed it was green when you were asking him—

Chairman LEAHY. No. His statement, which is part of the record, Senator Sessions, I was trying to give him a graceful way, rather than just saying, "You are way over time," and cut him off. But thank you for raising that point.

Senator HATCH. Well, Mr. Chairman, whether over or not, this is the Director of National Intelligence. We are all interested in what he had to say. I got the impression he was going through the history of this matter and was ultimately going to reach the points that you were concerned about and all of us are concerned about.

Chairman LEAHY. I will give the—

Senator HATCH. He ought to be able—

Chairman LEAHY. The Senator from Utah will have as many rounds as he wants, if he wants to have 20 rounds, to ask the Director those questions, we will give him those.

Senator HATCH. I would rather have him out watching over us from a security standpoint than here, to be honest with you.

Chairman LEAHY. Senator Specter.

Senator SPECTER. And now we return to Director McConnell. Going to the—if we could start the clock at 7 minutes, I would appreciate it.

Going to the three issues that you have raised, the surveillance of U.S. persons in the United States is now governed by the warrant procedure—

Mr. MCCONNELL. Yes, sir, it is.

Senator SPECTER.—applications of the FISA Court, probable cause.

Mr. MCCONNELL. Yes, sir. In all cases, yes.

Senator SPECTER. Before there was wiretapping or surveillance on a person in the United States, correct?

Mr. MCCONNELL. Yes, sir.

Senator SPECTER. You pick up the issue of compelling the private sector to help. We rejected the retroactivity of any such liability, but we have given you that assurance for the future, correct?

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

Senator SPECTER. Satisfactory. I think on our revisiting the statute we will not call for your certification, Mr. Director, which we did because of our concern about the then-Attorney General, but can lodge that in the Attorney General, we had some criticism that giving the authority for certification to the Director of National Intelligence, we were letting the fox guard the chicken house. And we did that because we trusted you as the prime assurance that we could go back to the Attorney General. That will be acceptable to you, won't it?

Mr. MCCONNELL. Yes, sir. I would prefer that.

Senator SPECTER. And when you pick up the issue of targeting foreigners overseas—I am going to get into some of the details, but first I want to be sure, Director McConnell, that we do not get into any areas which you think cross the line on secrecy which endangers our national security. Congresswoman Eshoo asked you in the House proceedings if you thought the congressional questioning of the administration's surveillance program would lead to the killing of Americans. And according to the record, you responded, "Yes, ma'am, I do."

Is that an accurate quotation?

Mr. MCCONNELL. Yes, sir, it is.

Senator SPECTER. Well, if we get into that territory, Director McConnell, tell us, and we will desist on a public session and undertake it in a private session to find out what we need to know.

But as I said in my brief introductory remarks, there is great value in telling the American people, to the extent possible, consistent with national security, what the threat is.

When you and I talked in July at length, there was public disclosure of the "chattering," which was similar to what had occurred prior to 9/11/2001, correct?

Mr. MCCONNELL. Yes, sir.

Senator SPECTER. To what extent can you say publicly the seriousness of the threat to U.S. national security?

Mr. MCCONNELL. The level of dialog and chatter increased significantly. We released, as you recall, a National Intelligence Estimate about the same time to try to capture the threat from that point 3 years forward.

Senator SPECTER. And what do you mean by "chatter"?

Mr. MCCONNELL. When we are observing activity of foreign targets, how they engage and what they are doing and what their planning might be and so on, we just refer to that as "chatter," indicating volume. So that level of volume had increased, and it caused us to be concerned.

We combined current activity with the assessment that I was about to mention that we completed after about a year of attempting to develop it and get it coordinated and so on. The timing of the assessment coming out is it was just ready in July; we did not speed it up or slow it down to meet any particular timeline. That is when it was ready. And what had happened is we had observed al Qaeda in the federally administered tribal area of Pakistan be able to re-establish a safe haven that allowed them to have the senior leadership recruit and middle-grade leadership recruit operatives and to train the operatives, and the operatives were being trained in things like commercially available components for explosives. And so that level of activity had increased significantly.

The intent of al Qaeda's leadership was to move those operatives from the training area into Europe and into the United States, and that was our concern, is our ability to recognize—

Senator SPECTER. What did you say with respect to moving that activity into the United States?

Mr. MCCONNELL. Operatives who were trained in a way to obtain commercially available explosives to then transit from the training region of—the border area between Afghanistan and Pakistan, to reposition. In some cases, they had recruited Europeans. Europeans in large part do not require a visa to come into this country. So purposefully recruiting an operative from Europe gives them an extra edge into getting an operative or two or three into the country with the ability to carry out an attack that might be reminiscent of 9/11.

Senator SPECTER. Anything besides the chatter and the activity in Pakistan which led you to believe they had the capacity to come into the United States, perhaps through Europeans who did not need visas? Anything beyond that that you can disclosed publicly?

Mr. MCCONNELL. I would rather not go too much further, but to answer a question raised by Senator Leahy earlier, I made references to some numbers. I learned long ago never use a number, so I violated my own rule. But about 50 percent of what we even know comes out of the FISA program. Within that, in answer to the Senator's question, when I said two-thirds, our ability within this 50 percent had been degraded by two-thirds because of the wording of the law, which had not been updated, leading up to this summer.

So the point I was trying to highlight, about 50 percent of what we know comes from this process; about two-thirds of that had been degraded. So my push and emphasis over the summer was we have to get this wording changed so we can be more efficient and effective in targeting foreigners overseas.

Senator SPECTER. Do the factors that were present in July which we discussed prevail today?

Mr. MCCONNELL. They do. One of our concerns has been the level of public activity. I do not know if you follow it that closely, but Osama bin Laden personally has now put out a video and two audio pronouncements over the last months or 6 weeks, and that is unusual. He had been absent from the airwaves for well over a year. So when we see that much activity at one time, our concern is it is a signal, it is an indication of activity. So while chatter continues, training continues, recruitment continues, I think probably the easiest way to capture the most recent events was the takedown in Germany of what is referred to as IJU, the Islamic Jihad Union, which is an affiliate group that trained in Pakistan with al Qaeda and trained the operatives that were arrested in Germany in Pakistan.

Senator SPECTER. I am going to come back in the second round to the question about giving the FISA Court authority when U.S. persons are targeted overseas instead of the Executive order, which now gives that to the Attorney General. I am going to come back to that to see if it would be acceptable. But I want to just close the loop on what you have just testified to by asking you how heavily do you weigh the Osama bin Laden public pronouncements where they disperse on video—how heavily do you weigh that as a threat and why do you weigh that as a threat?

Mr. MCCONNELL. Sir, it is one of many factors, and I would say it is a concern. It just causes us to be concerned and vigilant. These other factors that I mentioned are the ones that cause me greater concern. So you can look over time and a statement may or may not mean something. There are some who put more credence in it. So I would say I am concerned. But when I can see with sufficient detail recruitment and training and explosives design and that sort of activity, and you follow it over time, you would understand why we are concerned.

I would be happy to go into detail if we could go to a close session.

Senator SPECTER. Thank you.

Chairman LEAHY. Thank you, Senator Specter.

Of course, after this, if there are members who want a closed session on the Republican side, please talk with Senator Specter about

that. On the Democratic side, talk with me. And Senator Specter and I will consult and come to an agreement on that.

Senator Kennedy.

Senator KENNEDY. Thank you very much, Mr. Chairman, and thank you for having this hearing. Welcome.

Just to review old ground for a moment, in 1976, in the wake of the fact that we had widespread wiretapping during the previous administration, during the Nixon administration, then-Attorney General Levi, a Republican, with a Republican administration, asked a number of the members of this Committee down to the Justice Department' saying, "We have a real challenge to our national security." The challenge involved enormously sensitive information, not only with regard to embassies but with regard to matters that were taking place overseas as well. Enormously sensitive.

There was a sense that that Attorney General understood that the members of our Committee and the Members of Congress are as concerned about national security as anyone within the administration. And during that period of time, on four different occasions, members of this Committee went down to the Justice Department. And when the final legislation was enacted in 1978, there was one dissenting vote. One dissenting vote. We worked with a Republican administration and a Republican Attorney General to try and get the national security issues right.

Up comes Mr. Gonzales. The members of this Committee said—many of us who had been through the 1978 experience—"We want to work with you. We are as concerned about national security as you are." He said, "We do not need your help. We do not need your assistance. We do not need your involvement. And as a matter of fact, we are not even going to tell you what is going on."

Now, I want to have some idea which tradition you follow. Are you willing to work with this Committee? Do you have sufficient confidence that the members of this Committee are as concerned about security as you are and also as concerned about the rights and liberties of the American people, and that when we get it right from an intelligence point of view, we are going to get it right with regard to protecting our rights?

Mr. MCCONNELL. I do agree with that, Senator, absolutely.

Senator KENNEDY. Well, are you going to be working with this Committee?

Mr. MCCONNELL. Absolutely.

Senator KENNEDY. And can you give us the assurance that whatever is passed by this Committee is going to be the one and only limit in terms of intelligence gathering, that it is going to be the sole means by which the executive branch can intercept communications in the United States?

Mr. MCCONNELL. Sir, if we can get the law that we have just passed made permanent and address the other issues, then that is how I would intend to carry out this program.

Senator KENNEDY. This is the issue because there are members of the Committee who are not sure what the law is. You are going to explain in detail what the law is and what it covers, either in open or in closed session?

Mr. MCCONNELL. Yes, sir. I would be happy to do that.

Senator KENNEDY. Wholly and completely?

Mr. MCCONNELL. Wholly and completely.

Senator KENNEDY. Thank you.

Could I ask you a question about Attorney General certification and immunity from liability for carriers? Isn't it true that the carriers who act pursuant to a warrant or the Attorney General's certification already have immunity from liability?

Mr. MCCONNELL. I do not know the answer to that, sir. I could consult with counsel. I just do not know.

Senator KENNEDY. It is my understanding—I see your counsel that the carriers that act pursuant to a warrant or Attorney General certification already have immunity from liability.

Mr. MCCONNELL. Under the new law, that is correct. Yes, sir.

Senator KENNEDY. Well, it is true under the old law, too.

Mr. MCCONNELL. I do not know about the old law. What we asked for in the new one was to get—

Senator KENNEDY. OK. Well, if the warrantless surveillance program was legal, as you have claimed, what do carriers need immunity from?

Mr. MCCONNELL. I am not sure I understand your question, sir.

Senator KENNEDY. Well, if they have been abiding by the law, they should not need immunity. If they have been abiding by the Attorney General's certification, they should not need immunity. So why does the administration ask us to grant immunity for past activities when we have no idea what they were? At least I do not think any of the members of this Committee know what they were, but we are being asked to grant immunity, and that is what I am trying to drive at.

Mr. MCCONNELL. Going forward, there is proscriptive liability for anyone that would assist us in this mission. In a retroactive sense, those who are alleged to have cooperated with us in the past are being sued, and so it is to seek liability protection from those suits.

Senator KENNEDY. There is also a desire retroactively—to grant retroactive immunity.

Mr. MCCONNELL. That is correct, sir.

Senator KENNEDY. The point that is made is that this might bankrupt some of the companies if the lawsuits go ahead. It is a bad precedent, I think, if we finally have a law and then the carriers are able to violate the law and think that sometime in the future they can get immunity by talking about bankruptcy. There are alternative ways of preventing bankrupties. There are limits to damages, for example. But it is an important policy issue and question.

Let me be in contact with you about this so you have a full idea of what I am driving at, because it is complicated and I know that you want to get the right position on this.

Mr. Chairman, my time is just about up now. I will come back.

Chairman LEAHY. Thank you.

Senator Hatch.

Senator HATCH. Well, Admiral McConnell, the problem here is that there were legal opinions that warrantless surveillance could be undertaken, and these companies patriotically cooperated with the Government based upon those opinions. Is that a fair statement?

Mr. MCCONNELL. Yes, sir.

Senator HATCH. So the fact that there were no warrants because it was warrantless surveillance should not subject them to litigation.

Mr. MCCONNELL. Those that were alleged to have helped us were responding to requests from the Government that was official. Yes, sir.

Senator HATCH. Could you consider that response a patriotic response or—

Mr. MCCONNELL. Certainly, sir. Coming out of 9/11, you know, a lot of things happened where people wanted to be helpful and supportive and so on. So that is the period when it is in question. How would we understand and be able to push back this threat after the heinous events of 9/11?

Senator HATCH. Now, as you know, I am aware of what went on there because I was one of seven on the Intelligence Committee who were fully informed.

Mr. MCCONNELL. Yes, sir.

Senator HATCH. Were those activities helpful in helping to protect the country?

Mr. MCCONNELL. Yes, sir. They were essential. As I testified earlier, this process is a very, very significant part of our understanding of being able to warn—being able to see, understand, gain insight, and to be able to warn and prevent, move to cause things not to happen.

Senator HATCH. And to protect us as citizens in this country.

Mr. MCCONNELL. There have been a series of things that are not public. A few have become public, but there are many more that have not become public where we have been effective in shutting down something because of this program.

Senator HATCH. That is what the Protect Act is all about, is to allow you the ability to protect America in reasonable ways.

Mr. MCCONNELL. Yes, sir.

Senator HATCH. And we enacted it, and it passed somewhat overwhelmingly in the U.S. Senate.

Mr. MCCONNELL. Yes, sir.

Senator HATCH. But you do not have any axes to grind, do you? I mean, you are not really a political person, as I understand it.

Mr. MCCONNELL. No, sir, I am not. I mean, all I am attempting to do is to get the community positioned in the way that it can do its mission and then, consistent with the law, provide protection for citizens' privacy and civil liberties in the way that was captured in the original law in 1978.

Senator HATCH. Well, before the Protect Act, you were very concerned that you might not be able to protect the country. Is that correct?

Mr. MCCONNELL. We had lost two-thirds of our ability because of the change in technology and the wording in the law. Some have said, "Well, McConnell is blaming it on the FISA Court." I was not blaming it on any particular body. The wording in the law had not been changed. As has been noted, the law had been updated a number of times, but this problem had not been fixed. So what I was trying to flag is we need to fix that problem in the wording in the law so we can be effective in a foreign context.

Senator HATCH. In other words, before the Protect Act, the intelligence community tried to do what it could to protect our country, but there were issues raised up here and elsewhere, and a lot of complaining, and so we did the Protect Act to satisfy some of the criticisms and questions that were raised.

Mr. MCCONNELL. Yes, sir.

Senator HATCH. Is that a fair statement?

Mr. MCCONNELL. It is. Because of the change in technology, our access to communications, the place and the method because of the wording in the law would force us then to give Fourth Amendment protection to a foreign terrorist.

Senator HATCH. So without giving any classified information, would it be your opinion that we are still under onslaught with regard to foreign people who want to destroy our country or want to attack our country?

Mr. MCCONNELL. Sir, specifically they have al Qaeda and related—they have a program to acquire weapons of mass destruction, biological, chemical, radiological, or even nuclear. And if they obtain those materials, they intend to use them.

Senator HATCH. But it is even more than that, even general espionage and abilities to hurt Americans are still in play, aren't they?

Mr. MCCONNELL. Yes, sir, and that goes far beyond just the terrorists. I was just referring to terrorists.

Senator HATCH. So all you are asking for is the ability to be able to protect the people in this country.

Mr. MCCONNELL. Yes, sir.

Senator HATCH. And you are aware of an ongoing onslaught of efforts to try and hurt this country.

Mr. MCCONNELL. Indeed.

Senator HATCH. And to try and hurt our people. In fact, kill our people. Is that correct?

Mr. MCCONNELL. Yes.

Senator HATCH. This is not just some little itty—bitty problem, is it?

Mr. MCCONNELL. No, it is not.

Senator HATCH. It is widespread?

Mr. MCCONNELL. Yes, sir.

Senator HATCH. Now, a reading of the Protect America Act as enacted without knowledge of the rest of FISA and applicable Executive orders could be read to permit the targeting of U.S. citizens reasonably believed to be outside of the United States. Is that correct?

Mr. MCCONNELL. Sir, that assertion is made, but the mission of this community is foreign intelligence, and so if there was such targeting, it would have to be for a foreign intelligence purpose.

Senator HATCH. That is right. However, the intelligence community is bound by Executive Order 12333.

Mr. MCCONNELL. Yes, sir.

Senator HATCH. It is critical for the public to understand that you are still bound by that Executive order, and nothing in the Protect Act changed this. Is that correct?

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

Senator HATCH. Now, can you elaborate on the significant and necessary restrictions from Section 2.5 of this Executive order and

how they provide protection for the privacy of American citizens overseas?

Mr. MCCONNELL. Under 2.5, you would be required to produce probable cause standard. In this case, it is reviewed and approved by the Attorney General, and—

Senator HATCH. Well, that is a protection that you have.

Mr. MCCONNELL. Yes, sir. And the situation—just to get perspective, I think in the past year that happened 55 times, maybe 56, but in the 50s. And the situation was such that someone is either—they have been determined to be an agent of a foreign power operating with a foreign power or a terrorist, or in some cases that might be a dual citizen. So while someone has U.S. citizenship, they had foreign citizenship, too, so it would put it in that category where we would have to develop probable cause.

Senator HATCH. Other legislative proposals on this topic called for a narrow definition of "foreign intelligence information" applying only to international terrorism. Now, some have also called for a court order being required on foreign individuals overseas if a significant number of communications involve a person in the United States.

Now, would you provide an explanation of the flaws in both of these suggestions and how terrorists could adapt their behavior to trigger protections?

Mr. MCCONNELL. Yes, sir. As a practical matter, what you are able to do in this business is target one end of a conversation. You do that through a phone number or whatever. So the situation is we may be covering a foreign target in a foreign country. That person, we cannot control who calls them or who they call. If they call someone in the United States, now it sets up a situation where that could be the most important call, we intercept it because they could be activating a sleeper. It could be innocent.

Senator HATCH. By a "sleeper," you mean a sleeper cell of terrorists?

Mr. MCCONNELL. Sleeper cell, yes, sir. And it could be totally innocent. In the FISA legislation of 1978, we had similar conditions. Someone overseas could call into the United States. So the process that was actually adapted from a criminal wiretapping program called minimization was established in FISA, reviewed and approved by the court, so there is a minimization procedure. So if it is totally incidental, it would be taken—expunged from the data base. If it were activating a sleeper or terrorist related, it would be something we would be required to report foreign intelligence on. And if I might, if I could just take a minute, I want to just read from the joint congressional inquiry into 9/11, and I will just read a couple of passages:

"There were gaps between NSA's coverage of foreign communications and the FBI's coverage of domestic communications that suggest a lack of attention to the domestic threat. Prior to 9/11, neither agency focused on the importance of identifying and ensuring coverage of communications between the United States and suspected terrorists located abroad." That is exactly what happened with some of the terrorists here that were calling known terrorists overseas, and we missed that information.

The joint congressional inquiry concludes, "The Joint Inquiry has learned that one of the future hijackers communicated with a known terrorist facility in the Middle East while he was living in the United States. The intelligence community did not identify the domestic origin of this communication prior to 9/11 so that additional FBI investigative efforts could be coordinated."

So what we are describing here in this joint commission was a review after the fact of what we should have done, and the argument that I am making for the Committee today is preserving the legal foundation for us to target foreigners, foreigners that might call into the country to activate a cell, or a cell that is in the country reaching out to coordinate with a foreign terrorist cell located overseas. So our community is only targeting the foreigner overseas.

Now, some will say, well, wait a minute, there is a situation where you could target overseas when your real target is in the United States. That is a violation of the Fourth Amendment. It is unlawful. So in that case, if we wanted to target or needed to target somebody in the United States, we get a warrant.

And so from the way I think about it, it leaves the flexibility to our foreign intelligence mission. We have a situation under the law to deal with a foreign threat in the United States, and that is all warranted coverage.

Senator HATCH. My time is up, Mr. Chairman.

Chairman LEAHY. Thank you.

Senator Feinstein.

Senator FEINSTEIN. Thank you very much, Mr. Chairman.

Welcome, Director McConnell.

Mr. MCCONNELL. Thanks, ma'am.

Senator FEINSTEIN. I have a series of questions. I believe that the FISA Act, since its passage in 1978, along the lines that Senator Kennedy was speaking, has been the exclusive legal means for conducting electronic surveillance for intelligence purposes. Do you agree that FISA, as presently written, includes language that it is the exclusive means to conduct surveillance for intelligence purposes?

Mr. MCCONNELL. Senator, you and I have discussed this before.

Senator FEINSTEIN. Right. I just want to go on the record with what you said to me.

Mr. MCCONNELL. Yes, ma'am, and—this is how I would execute this authority under the authorities that I hold. But what you are addressing is a constitutional issue, the difference between Article I and Article II—

Senator FEINSTEIN. What I am asking for is a yes or no—

Mr. MCCONNELL. But I can't—ma'am, I can't commit one way or the other to a debate between the executive branch and the legislative branch. Under my authority, we get this law positioned right, that is how I would cause this community to execute our authorities. So I would be consistent with this law. But I can't solve the constitutional debate that your question is addressing at a fundamental level.

Senator FEINSTEIN. OK. Senator Hatch mentioned Executive Order 12333, Section 2.5, which we have talked about previously. This section applies to any time the intelligence community tries

to get information about a U.S. person overseas and requires that the Attorney General make a prior finding that there is probable cause to believe that the U.S. person is an agent of a foreign power.

Would you agree to putting the language in Section 2.5 as currently written into statute?

Mr. MCCONNELL. Ma'am, I wouldn't object. What I would ask is we receive the language and examine it across the table from each other to understand its impact. And so long as it does not have unintended consequences, I would have no objection.

Senator FEINSTEIN. For the subset of Section 2.5, operations where the collection is done inside the United States, would you support shifting the probable cause determination from the Attorney General to the FISA Court?

Mr. MCCONNELL. It is inside the United States, ma'am. Even today it is under the FISA Court.

Senator FEINSTEIN. Thank you very much.

Now I would like to ask some questions of minimization. Do the minimization procedures prevent NSA from retaining communications that do not contain foreign intelligence information?

Mr. MCCONNELL. If recognized, minimization would require them to expunge it from the data base.

Senator FEINSTEIN. Do the minimization procedures require that U.S. person information is made anonymous before it is disseminated as intelligence reporting?

Mr. MCCONNELL. Yes, ma'am, it does.

Senator FEINSTEIN. Is it required that a warrant be obtained when the U.S. person themselves becomes the subject of interest?

Mr. MCCONNELL. Yes, ma'am, and located inside the United States, yes, always.

Senator FEINSTEIN. And the finding is of intelligence value. Is that correct?

Mr. MCCONNELL. Back on the minimization procedures, let me give you an example, if I may. If two foreigners are discussing a member of this body, we would have—that is a U.S. person, so we would have to determine how we would deal with that. So if it had foreign intelligence value, you are being targeted or whatever, it is our obligation to report that. So we would report it as U.S. Person 1, or say it was the second person involved, U.S. Person 2. So the attempt is to protect the identity of the U.S. person when it is done in a foreign intelligence context.

Senator FEINSTEIN. All right. Let me just clarify that. When the pick-up is being analyzed and a determination is made that there is intelligence value by the analyst, exactly what happens?

Mr. MCCONNELL. The report would be written, and the identity of a U.S. person would be, as I mentioned, listed as U.S. Person 1, U.S. Person 2.

Senator FEINSTEIN. And then what is the warrant?

Mr. MCCONNELL. If for whatever reason the U.S. Person 1 or 2—say they were terrorists and they become a subject of a target or a subject of surveillance, then we would be required to get a warrant.

Senator FEINSTEIN. And does that happen when the finding is by the analyst that the individual is of intelligence value?

Mr. MCCONNELL. It would always happen that way. Think of it this way—

Senator FEINSTEIN. So that is the trigger.

Mr. MCCONNELL. It is what do you target. If you target—think of it as a phone number. If you put that phone number in the data base as a target, you would have to have a warrant.

Senator FEINSTEIN. All right. And that is determined, as I understood it previously, when the analyst makes a finding that there is intelligence value.

Mr. MCCONNELL. That is a way to phrase it. Let's just use a sleeper cell as an example. A foreign terrorist, which is your target, calls into the country and makes contact with somebody who is an accomplice or maybe a sleeper. At that point you would flag that information for the FBI so the FBI could get a warrant to conduct surveillance of that person.

Now, let's suppose that it is a foreign target, they call into the United States, and it is Al's Pizza Shop, and it has nothing to do with anything. You would take that information out of the data base. You would expunge it from the data base.

Senator FEINSTEIN. Would you support a provision that required the Government to submit the minimization procedures it uses for the Protect America Act collection for FISA Court review, not afterwards as in the Protect America Act, but before?

Mr. MCCONNELL. They already have done that, and I wouldn't have any objection to them looking at the process and—

Senator FEINSTEIN. If that were written into the law.

Mr. MCCONNELL. Yes, ma'am. But, now, I have to take it one step further because we get into unintended consequences. Depending on the phrasing and the way it is captured in the law, it could put us in a position that we couldn't do foreign surveillance because we can't tell who that person is going to call, we can't control that until we got review beforehand. So if it is interpreted that way or could be interpreted that way, it would cause us great difficulty.

So I am not objecting to how you phrased it, but we would have to look at it in the context of the bill and how might it be interpreted, because here is the thing I can't recommend we do, and that is, introduce uncertainty or ambiguity that would cause us to lose effectiveness. Because we are talking about people who are planning and operating in minutes or hours as opposed to long lead times.

Senator FEINSTEIN. Let me summarize it, and we have talked about this before. But it is my position that any collection against a U.S. person abroad with the minimization process, that that process should be approved by the court prior, and you have agreed to that, and that—

Mr. MCCONNELL. Ma'am, you just mixed two things. That is why this gets so complex.

Senator FEINSTEIN. How have I done that?

Mr. MCCONNELL. All right. You went from targeting a U.S. person abroad to minimization. Two different issues.

Senator FEINSTEIN. A U.S. person abroad is minimized.

Mr. MCCONNELL. No, ma'am. Let's say a U.S. person abroad is a dual citizen, agent of a foreign power. Currently, what the Executive order says is the community would have to produce probable

cause standards information, but you take that to the Attorney General for a warrant.

Now, if you are—

Senator FEINSTEIN. I am not talking about that part. I am talking about an innocent U.S. person abroad that gets caught up in one of these calls and how that call is minimized.

Mr. MCCONNELL. All right. So we are talking about inadvertent collection.

Senator FEINSTEIN. That is correct.

Mr. MCCONNELL. Now, what is the question? Am I objecting to—

Senator FEINSTEIN. So what is the minimization process and how does it function and what happens with that collection?

Mr. MCCONNELL. First of all, you may not even realize it is in the data base, because if you do lots of collection you have to have a reason to look. You look at it. If it is foreign intelligence, then it is treated the way we discussed. If it is now recognized it is incidental, it would be expunged from the data base.

Those procedures have been reviewed by the FISA Court. I would have no objection to them looking at them again.

Chairman LEAHY. Senator.

Senator FEINSTEIN. My time is up. Thank you.

Chairman LEAHY. It is, and Senator Coburn is next.

Senator COBURN. Thank you, Mr. Director, for being here, and thank you for your service.

I just want to spend a little more time giving you a chance to outline for the American public the assurance that we have a minimization program that has been looked at, the procedures for that have been looked at by the FISA Court, agreed to by the FISA Court, and the assurance that you can give the American people that, in fact, there is not going to be a violation of that minimization process. Can you speak to that for a moment?

Mr. MCCONNELL. Yes, sir, I can. We have been doing this for 29 years. It is reviewed at four tiers, four different levels. The agency doing it, they have a training process inside, and it is looked at by their general counsel and their IG. My office, as the overseer of the community, we review it. The Department of Justice also reviews it. The FISA Court reviews it for the process and so on, and then it is subject to review by the Congress and the oversight committee.

So if there is a question and they want to look at, you know, what we have done or what the procedure—or visit NSA or look at any of that, we would make it all available so people could see it and understand it.

Senator COBURN. OK. So that brings me to my next question. You all do not operate without oversight, correct?

Mr. MCCONNELL. No, sir, we don't.

Senator COBURN. There is oversight. And what are the committees of Congress that have oversight over what you do?

Mr. MCCONNELL. Primarily, it is the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.

Senator COBURN. OK. Can you kind of give us a short summary of the oversight mechanisms of the Protect America Act that are in place today?

Mr. MCCONNELL. Yes, sir. The four tiers I just mentioned: internal, the agency; external, meaning my office and the Department of Justice; the FISA Court; and the Congress. Since the law was passed in August, and we put our—we came back up on our full coverage, there have been approximately ten visits out to NSA to sit down with the analysts and look at the data and the process and what is the training standard, what are the conditions, and what would you do with the information and track it through the process.

So it has been extensively reviewed, and it is subject to that extensive review so long as there is a question, or if anybody wants to revisit on a periodic basis.

Senator COBURN. OK. One of the questions—and I think legitimately raised, especially because of some of the past actions—is developing the trust of the American people. There is a certain paranoia out there because we are close to stepping on individual American rights.

Do you as an agency have plans to try to communicate in a positive fashion both to the Congress and the American people about holding your responsibility for both minimization as well as the protection of individual rights in this country?

Mr. MCCONNELL. Yes, sir. I personally have been very, very public on this issue, criticized in some cases for being so public. But if you will remember the three points that I started with—no warrant for a foreigner overseas, a foreign terrorist located overseas; a way to get assistance from the private sector. The third point is the one I believe very, very strongly in. Anytime there is surveillance of a U.S. person where that person is the target, I support, believe in, and would strongly endorse that we have a warrant. That warrant is given to us by a court, and that is not a menial process to go through because it is probable cause standard. Some would argue, well, you can go really fast because in an emergency you can get just a phone call, but you are still meeting a probable cause standard.

So the Director of NSA, me, the Attorney General, we are not going to go fast until we have the facts in front of us, because it ultimately has to withstand the scrutiny of a court.

Senator COBURN. So let me summarize, and you say if you agree with this. If you are an American citizen, you are not going to be targeted to any of this without the approval of a court.

Mr. MCCONNELL. That is correct.

Senator COBURN. All right. That needs to be said, loud and loud and loud. If you are an American citizen, you have the protection of a court before you are subject to this law.

Mr. MCCONNELL. If you are an American citizen or even a noncitizen in the country, you have the protection of a warrant issued by a court before we could conduct any kind of a surveillance.

Now, sir, so you are aware, some will argue that we are targeting overseas and the person overseas calls into the United States. That is where minimization starts. We cannot control what the overseas target does. We have to have a process to deal with that, and that is where minimization was introduced. It is an elegant solution. We have tried every way we can think of to make that different or stronger or more complete, and those who framed this law in 1978

and all of us that have looked at it since, we can't find a better process.

Senator COBURN. But those minimization procedures, like Senator Feinstein suggested, have been looked at by the FISA Court.

Mr. MCCONNELL. They have.

Senator COBURN. And you are suggesting and you would be happy to have those reviewed.

Mr. MCCONNELL. Yes, sir.

Senator COBURN. And those probably should be reviewed sequentially and annually.

Mr. MCCONNELL. By not only the court, but by the Congress.

Senator COBURN. Right.

Mr. MCCONNELL. In whatever periodicity they need to review them to be comfortable we are doing it the right way.

Senator COBURN. I have no other questions.

Chairman LEAHY. Thank you very much, Senator Coburn.

Senator Cardin.

Senator CARDIN. Thank you, Mr. Chairman.

Admiral McConnell, I very much appreciate your service to our country, and I can tell you that we all agree that we need to make sure that our intelligence community can get the information they need for protecting the civil liberties of the people in our country. We also agree we need to modernize our laws and gather intelligence information.

But let me just suggest that I have confidence in your administration of the agency, but the laws that we create today are going to go well beyond your term in office. So we need to make sure that we have the right laws in place. I agree with Senator Specter's observations that some of the administrative decisions should be placed in statute in order that we have the protection, and I think that is a good suggestion that was made by Senator Specter.

I appreciated also your analysis of the law in the 1970s. This is not paranoia. In the 1950s and 1960s, we had serious problems dealing with the civil liberties of the people in this country, and the FISA Court law was developed in order to provide the right balance. And as you point out in your testimony, you agreed with that law at its time, but it needs now to be modernized.

Well, I think we still have concerns today, and I just really want you to focus a little bit more on the responsibilities for check and balance in our system. Traditionally, in criminal investigations, in the work of the Department of Justice, the courts have been the body that we look to as the check and balance. And yet the bill that was passed in August allows the FISA Court to look at the procedures used in gathering information, but it cannot be set aside unless it is clearly erroneous.

Now, you do not need to be a lawyer to know that is a pretty difficult standard for the Court to use to set aside the procedures that have been developed. We are talking about the civil liberties of the people in this country. It seems to me that is a pretty tough standard for the entity, the branch of Government that is supposed to be our checks and balance. In order to get involved and suggest changes, they would have to find that your procedures are clearly erroneous.

Your comments on that?

Mr. MCCONNELL. Sir, the target that you are describing is foreign. It is not a U.S. person. So the procedures we are talking about—

Senator CARDIN. But it has been pointed out before that in that process there is very likely at times to be communications with U.S. citizens. So there is the information being gathered potentially involving U.S. citizens.

Mr. MCCONNELL. The procedures in question you are describing are the procedures to determine foreign-ness—that is an odd term, but it is how do we know that the person being targeted is foreign. So it has a foreign context.

Now, as we discussed with minimization, if you are targeting that foreign person in a foreign country, you cannot control who they might call. That is where minimization comes in. If the foreign terrorist calls into the United States, what do you do with that call?

Since we cannot determine ahead of time who they might call, some say, well, it is easy, just make it foreign to foreign. You can only target one thing at a time, and while the vast majority—the vast majority—of the time it is foreign to foreign, in that isolated instance when it might be foreign to U.S., how do you deal with it? And that is the elegant solution that was captured in 1978, and all I am arguing is return us to 1978.

We had this same debate and situation in 1978 when the means of communication was wireless. The only thing that has changed, it went from wireless to wire. So that is why we found ourselves in this box.

Senator CARDIN. I guess my point is this: You make a very persuasive argument that to require an individual application to the FISA Court on a case involving a foreign person would be too onerous and be ineffective in getting the information. So Congress is looking at saying, OK, rather than the individual case, take the process that you are using to the FISA Court and have more involvement of the FISA Court in the process.

I am not sure we got it right—in fact, I do not believe we got it right in the last bill we passed as to the appropriate balance between the FISA Court and your work on approving the procedures that are used.

I guess my question to you is: Do you have any suggestions to us how we could set up a more effective involvement of the FISA Court on the procedures that you are using that will give more comfort that we have in place the appropriate checks and balances without compromising the ability of your agency to go after the individual that you believe you should?

Mr. MCCONNELL. I have no objection to working out the best possible solution, so I would be happy to work in any way—and I would even suggest perhaps we ought to involve the FISA Court in that discussion so that we can get the right balance between being effective in the foreign intelligence mission and protecting civil liberties.

What I am worried about is because we were in a time crunch before, we are in a situation where words were about to be put into law, which is very difficult to back away from, that would have in-

troduced uncertainty that I feel confident would have inhibited our effectiveness.

So we are happy to look at anything, just let's sit down and examine what do you think that means and the 20 lawyers I have working this that are expert in it, what do they think, and what is the right balance.

Senator CARDIN. That is a fair enough challenge. I would just submit that we have a couple months now before the deadline approaches, and it would be useful if we have a meeting of the minds, if that is useful to try to improve the checks and balances through the FISA Court on process. Your suggestions or your attorney's suggestions in that would certainly be a good starting point for us in doing that. And it would be helpful if we could get that information to our Committee.

Thank you, Mr. Chairman.

Chairman LEAHY. Senator Sessions.

Senator SESSIONS. Thank you.

Thank you, Admiral McConnell, for your work and service to America and for protecting America, and I know that every morning you get up and until you go to bed at night, you worry about how to preserve this country and to make sure that another 9/11 does not happen. But the threat is out there. You have made that clear.

There was a national consensus after the attack on 9/11—and the 9/11 Commission was part of that and concluded that intelligence is the critical thing to preserve the safety of the people of the United States. Isn't that correct?

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

Senator SESSIONS. That is your business, but there is no way that we can stop everybody coming into America, we can stop every dangerous act that occurs, but knowing who has a malicious intent, intelligence, is the key to protecting us. Would you not agree?

Mr. MCCONNELL. Yes, sir. I do agree with that.

Senator SESSIONS. Well, I have been frustrated because it seems to me the tenor and tone of hearing after hearing after hearing since 9/11 has been that somehow what you are doing is an attempt to constrict the great freedoms that Americans believe in, and we have forgotten the dangers that we face. And I would just note with regard to 1978, nobody denies that the people in 1978 were striving as best they could to correct some abuses that had occurred. But they created a wall of separation between the CIA, foreign intelligence and domestic intelligence, and the 9/11 Commission concluded that was a disaster.

Mr. MCCONNELL. Yes, sir.

Senator SESSIONS. And we reversed that, clearly, promptly, when we faced up to what the good-intentioned people did in 1978.

Also, in 1978, through good intentions, they prohibited intelligence officers from undertaking operations and informant relationships with people around the world who may have had bad records. Do you remember that?

Mr. MCCONNELL. Yes, sir, I do.

Senator SESSIONS. The intelligence community was concerned about that at the time, but Congress did not listen, and we did that. And after 9/11, that wonderful idea was examined in the cold

light of day and promptly changed and eliminated. So our danger, I would submit to my colleagues, is that through good intentions we can create laws that, in fact, inhibit the legitimate ability of this Nation to protect itself.

Now, having been through this, and having had, in 12 years as United States Attorney, I think one or two wiretaps, I know a little bit about that. And let me just ask you: You are not a lawyer, Admiral.

Mr. MCCONNELL. No, sir.

Senator SESSIONS. You are doing pretty well for a non-lawyer, I have to tell you. But when you obtain a wiretap in the United States on an American citizen, it takes a good deal of effort to do that. But once you obtain the ability through a court order at great effort, then you—you don't just—a person doesn't just talk to himself on the phone. You listen to who the person talks to.

Mr. MCCONNELL. Yes, sir.

Senator SESSIONS. So once you have a lawful intercept, a lawful wiretap on an American citizen, you listen to who they call. Likewise, if you have a lawful intercept on a foreign person, you listen to who they talk to.

Mr. MCCONNELL. Yes, sir.

Senator SESSIONS. Isn't that right?

Mr. MCCONNELL. That is correct.

Senator SESSIONS. So if they happen to call not a foreign person but call somebody in the United States, then that is expected, to me, from the beginning that they might do that, and you would want to listen to that conversation.

Mr. MCCONNELL. Yes, sir.

Senator SESSIONS. I do not see that fundamentally that is any different than the principle I have referred to about a lawful warranted wiretap here.

So you listen to people who call, but if they call an American citizen and it appears that that conversation is unrelated to terrorism, or it appears to be innocent, then you even take steps to minimize that conversation.

Mr. MCCONNELL. Yes, sir.

Senator SESSIONS. Is that right?

Mr. MCCONNELL. That is correct.

Senator SESSIONS. And how do you do that, again?

Mr. MCCONNELL. It is just expunged from the database.

Senator SESSIONS. Well, isn't that a bit dangerous? What if they were using code? Are you taking some risk there? Because if they were using some innocent code and you even take the name of the person they called in the United States out of the system?

Mr. MCCONNELL. Yes, sir. That is a judgment call. There would be some potential risk.

Senator SESSIONS. But as an effort to avoid criticism from those who always seem to be unhappy with what you are doing, you have gone to the extent that you would minimize that call by removing the name from the system.

Mr. MCCONNELL. Yes, sir.

Senator SESSIONS. Now, let me ask you, if a person has been identified to be associated with a terrorist organization, they are somewhere in the mountains of Afghanistan, and they are calling

someone in the United States talking about a meal or what kind of television set they have and it seems to be innocent, do you still minimize that call?

Mr. MCCONNELL. We would. It would be a judgment call. We would hope we would have continuity on the person we are targeting, so if we had some reason to believe—and let's suppose that a discussion about a meal could be interpreted about planning for an operation. At that point, one, you would report the information; and, two, if that person, the U.S. person in the United States, you would coordinate with the FBI then to get a warrant against that person to find out if it was, in fact, terrorism related.

Senator SESSIONS. But you would not have a basis to get a warrant based on what appeared to be an innocent phone call, factually, and so the only connection you have is that somebody in the United States is talking to a terrorist.

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

Senator SESSIONS. And you are minimizing that.

Mr. MCCONNELL. Right.

Senator SESSIONS. Unless it appears that the conversation had some relationship to what might be unlawful activity.

With regard to Senator Leahy's comment suggesting that you misstated the impact of the FISA law, I would like to give you a chance to explain that again. I thought your explanation made a lot of sense to me. Anybody can make a mistake. But I think your testimony was quite accurate as you understood it. Would you explain that?

Mr. MCCONNELL. Yes, sir. I have used some numbers a couple times. Someone had asked me what is the significance of this program, and the point I was trying to make, it is probably somewhere in the neighborhood of 50 percent or more of our total collection to understand this threat.

Once you take FISA as a stand-alone, people had asked me, well, what had happened with the wording under the old law based on subsequent reviews by the FISA Court, and the answer I gave is that we have been reduced by about two-thirds of what our capabilities were over that period of time. So we were getting into an extremist situation. Known terrorists overseas, we were unable to target without a probable cause level one. Probable cause is a hard standard to satisfy, and so it takes time. So working those off, we started in the spring to try to work them off, and, in fact, over the summer we were falling further and further behind, because there are lots of potential targets, and a single target, single human being, could use multiple avenues of communication. So you find yourself trying to catch up. That was the first problem.

Second is the very people who can understand this, the ones who speak the language, that know the individuals in a terrorist cell, are the ones that have to stop and do the justification. And so we actually had a situation where management of the process would have to make a judgment: Do I stay on target with the one or two or three or four that I have warranted coverage of? Remembering this is a foreign target in a foreign place? Or do I stop and give up on that target while we spend time writing a justification?

Senator SESSIONS. To get a probable cause for a warrant that probably takes a hundred or more pages chock-full of facts and fig-

ures is very difficult to write, and if you are in error, the law officer will be accused of perjury. So they have to do it right, and it takes a lot of time.

Mr. MCCONNELL. Yes, sir.

Senator SESSIONS. Thank you, Mr. Chairman.

Chairman LEAHY. Senator Feingold.

Senator FEINGOLD. Thank you, Mr. Chairman.

Thank you for coming before the Committee, Mr. Director. I would like to start by following up on Senator Kennedy's questions about the retroactive immunity you are seeking. How can members of this Committee evaluate that request without facts about the alleged conduct in question?

Mr. MCCONNELL. Sir, those facts should be available to you. What I am asking for in a broad context—there are those who are alleged to have cooperated with us, that could be and are being subjected to suits. So in this context of doing this mission, when you understand the technology of today and how the ebb and flow of what it is we have to use to do our mission, we can't do it without the cooperation of the private sector. The United States intelligence community cannot do this mission without the cooperation of the private sector.

So in the situation we found ourselves in, the law of last month talked of proscriptive protection. What I am asking for is we still have this situation to deal with retroactively. So I am asking for us to consider that in the deliberations you have. If there is information that you need to do that, I will make every effort to get you whatever I can—

Senator FEINGOLD. You have refused to provide Presidential authorizations and DOJ opinions—

Mr. MCCONNELL. No, sir, I haven't refused.

Senator FEINGOLD [continuing]. That I think are critical to understand this.

Mr. MCCONNELL. I haven't refused to provide the Committee with anything. I am in a position where I am attempting to conduct a mission. The administration that I work for, I have had some dialog about how that might play out. As I understand it, there is a negotiation between the Chairman and those in the White House about how this might play out. So I have made my recommendations, but I don't control the process.

Senator FEINGOLD. Well, I think that is critical, and I would say that—

Chairman LEAHY. Without going into the Senator's time, and your recommendation was what?

Mr. MCCONNELL. We need to provide the appropriate level of insight and information for the Committee to get us to the place where we can get the right legislation for this mission going forward.

Senator FEINGOLD. Does your recommendation include Presidential authorizations and DOJ opinions?

Mr. MCCONNELL. Sir, I don't want to go into that level of specificity.

Senator FEINGOLD. I would really suggest that if you are serious about this immunity proposal, which you obviously are, you have to make sure that Congress has what it needs to evaluate it. That

is just a bare minimum for us to be able to do our job. You have a job to do, and you are trying to do it well.

Mr. MCCONNELL. Yes, sir.

Senator FEINGOLD. We want to be in the same position.

Mr. MCCONNELL. I understand.

Senator FEINGOLD. The only way we can be in that position is if we have the material so we can understand this.

Let me ask you, as a general matter, do you think that private sector liability for unlawful surveillance plays any role in the enforcement of U.S. privacy laws and in providing disincentives to engage in lawful behavior?

Mr. MCCONNELL. That is a pretty complex question. In there you have said "unlawful." I am not suggesting anything, endorsing anything that is unlawful. So could you—

Senator FEINGOLD. Well, I think it is pretty simple. Do you think there is a role for private sector liability to make sure that people's privacy is protected in this country? Do you believe in that principle?

Mr. MCCONNELL. I believe that the process should be subjected to the appropriate legal framework so that privacy is protected. Yes, sir, I do agree with that.

Senator FEINGOLD. You and Mr. Wainstein have stated several times in hearings over the last couple of weeks, and I think you said it again here today, that you would be willing to look at language proposed by Members of Congress for changes to the Protect America Act, but that you, of course, want to be careful to ensure that there are not unintended consequences that result from what may seem like small changes in the language.

Mr. MCCONNELL. That is correct.

Senator FEINGOLD. I take your point. But the point I want to emphasize here is I think that obligation goes both ways. Congress has to be careful also not to unintentionally authorize activities that we do not want conducted. I know there has been some back and forth about this. You are very familiar with the controversy surrounding the language in the PAA authorizing acquisition of information "concerning" persons outside the United States. Why was this word "concerning" used? And why should Congress even consider reauthorizing such broad and ambiguous language?

Mr. MCCONNELL. Sir, I talked to the keeper of the pen when that was drafted, and, quite frankly, we were not sure why the word "concerning" was used. Different language—at one point it was "directed at," at another it was "concerning."

So the message I would deliver today is let's get the language that we can agree to, examine it from the responsibilities of the Congress and the responsibilities that I have to do this mission, and play it out to see what does it mean and how might it be interpreted so we can get to the right language. So if "concerning" is the wrong word, let's agree to a better word.

Senator FEINGOLD. The funny thing about this is we are not talking about a proposal. This is the law of the land. And this underscores the problem with this rush to judgment that we had in the last-minute push to get this bill passed, if you were not even comfortable with this language. And I have to say that we have to be a little worried about this sort of thing because this is the same

administration that claimed in one of the most absurd legal arguments I have ever heard that the authorization Congress passed to use military force in Afghanistan after 9/11 somehow allowed it to wiretap Americans in the United States without a warrant, and they did so for years in secret. So when members of the administration say that we should more or less trust them with something like this members of the public and the Congress have every right to be skeptical—and we have a duty to be skeptical. But I do appreciate the fact that you have acknowledged that there are concerns with the word "concerning" and that we have to take it seriously.

Director McConnell, you stated that reverse targeting is a violation of the Fourth Amendment and grounds for criminal prosecution. In public testimony to the House Intelligence Committee last Thursday, Assistant Attorney General Wainstein stated that reverse targeting includes wiretapping an individual overseas when you really want to listen to the American with whom the target is communicating. Do you agree with that description?

Mr. MCCONNELL. I do.

Senator FEINGOLD. And is this something that is essentially self-policing? How does the executive branch ensure that this constitutional principle is not violated?

Mr. MCCONNELL. As I tried to explain before, you can only target one thing, and so if the U.S. person in this country, for whatever reason—terrorists or whatever the issue is—becomes a target, then you would be required to have a warrant.

Now, if you engaged in that process of reverse targeting where you are targeting someone overseas and your real target is in the United States, that would be a violation of the Fourth Amendment. That is unlawful.

Senator FEINGOLD. Last Thursday, you told Congresswoman Schakowsky that while you do not know how much U.S. person information is in your databases, you could provide information about how much U.S. person information is looked at and how much is disseminated. Can you do that with regard to these new authorities? And when can you make that information available to this Committee?

Mr. MCCONNELL. The information is being prepared now, and, yes, I can do it with regard to the new authorities.

Senator FEINGOLD. And when can we receive that?

Mr. MCCONNELL. I don't know what—I have tasked it. I am waiting for a response back. I don't know yet. As soon as I know, I will be happy to advise you.

Senator FEINGOLD. Days? Weeks?

Mr. MCCONNELL. I would say weeks.

Senator FEINGOLD. During a hearing of the House Intelligence Committee, you stated that the bulk collection of all communications originating overseas "would certainly be desirable if it was physically possible to do so," but that bulk collection of communications with Americans is not needed.

Is bulk collection of all communications originating overseas, including communications of people in the United States, authorized by the Protect America Act?

Mr. MCCONNELL. It would be authorized if it were physically possible to do it. But the purpose of the authorization is for foreign intelligence. So when I say—

Senator FEINGOLD. So there is nothing, there is no language actually prohibiting this?

Mr. MCCONNELL. So long as it is foreign, in a foreign country for foreign intelligence purposes.

Senator FEINGOLD. Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

Before Senator Whitehouse starts, I am just curious. In listening to your answers to Senator Feingold's questions, this retroactive immunity basically takes away rights of plaintiffs who have spent money on suits and so forth. They may not be successful if they went through the courts, but it is taking away all their rights. And I have heard so many speeches from my good friends on the other side of the aisle, everything from environmental laws on, as being illegal takings. Was this a taking?

Mr. MCCONNELL. I don't know what you mean by "taking."

Chairman LEAHY. Well, if we take away somebody's rights to have a suit, we do it retroactively, we do it without any compensation. I just throw that out. Your lawyers may want—don't you try to answer, but it is interesting if we are talking about environmental law, it is terrible that we would consider this because it is a taking. But if we want to remove somebody's rights to a suit, it is not.

Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Mr. Chairman.

Admiral, good to see you again.

Mr. MCCONNELL. Thank you, sir.

Senator WHITEHOUSE. Some of what we are going to discuss will be well-plowed ground between the two of us because we have had these discussions in closed sessions. But I think it is important to go over it again in a public session because it is my very, very strong belief that the problems that we face in adapting the Protect America Act to protect American citizens are very solvable. And had it not been for the atmosphere of stampede that was created in the waning days of the session and had we had a little bit more time to talk coolly with one another, we could have solved it working off a very sensible template, which is Title III surveillance that takes place in the United States right now, such as the Senator from Alabama mentioned a moment ago.

In that context, it is my understanding that there are basically two categories of surveillance of Americans that are of concern under the Protect America Act. One is the surveillance of an American when they are abroad, and the second is the surveillance that is incidental to the intercept of a target abroad when they happen to speak to an American. Can we talk about them in those general two categories?

Mr. MCCONNELL. Yes, we could, in a foreign context. Of course, if it is in the United States, it is—

Senator WHITEHOUSE. That is a different issue. That is covered by existing law.

Mr. MCCONNELL. Right.

Senator WHITEHOUSE. Under the Protect America Act, there is no court warrant that is required for a person reasonably believed to be outside the United States. That is the magic phrase in the statute, correct?

Mr. MCCONNELL. That is correct.

Senator WHITEHOUSE. And if you look just at the language in the statute alone, a person reasonably believed to be outside the United States could be an American traveling on vacation, somebody visiting family in Ireland, somebody on a business trip. It could even mean troops serving in Iraq right now. Correct?

Mr. MCCONNELL. You could interpret it that way.

Senator WHITEHOUSE. And the protection against it being interpreted that way is an Executive order that requires the Attorney General to assure that the target is an agent of a foreign power. Correct?

Mr. MCCONNELL. That is correct.

Senator WHITEHOUSE. Now, the domestic model for this kind of surveillance requires, very consistently with the American system of Government and the separation of powers, that a court get involved and that the executive branch, the FBI, for instance, does not get to make that determination on its own.

Mr. MCCONNELL. Yes, sir. But what you just shifted to was a domestic situation where you have a warrant. And what I would highlight is in the vast majority of the situations that would involve this community, we are targeting a foreigner for which there is no warrant. So it is a little bit—

Senator WHITEHOUSE. I agree, but I am talking about where you are targeting an American who happens to be abroad. That is the category we are talking about here.

Mr. MCCONNELL. OK.

Senator WHITEHOUSE. In that category, as I understand it, you have agreed that the Executive order, assuming the language is all appropriate and does not create unintended consequences, could be codified in this statute. Would you also agree that the determination whether the person is an agent of a foreign power could be a FISA Court determination rather than a determination within the executive branch?

Mr. MCCONNELL. Sir, that is a possibility, and as we discussed the last time we talked about this, it sounds reasonable here at the line of scrimmage. But let's see the language and examine it, make sure it says what you want it to say and doesn't impact us in some way that causes a loss of flexibility. And given it doesn't have unintended consequences, I personally would have no objection to that.

Senator WHITEHOUSE. And would you agree at least that by bringing in the FISA Court we are matching, in the context of an American who happens to be abroad, the type of procedural protection that an American enjoys when they happen to be in the United States?

Mr. MCCONNELL. I would.

Senator WHITEHOUSE. OK. The other issue is the incidental intercepts, and as Senator Sessions pointed out, those happen all the time. Like him, I have obtained wiretaps before, both as United States Attorney and Attorney General. In fact, as Attorney General I had to do it myself personally with the presiding judge of the su-

perior court because Rhode Island is careful about letting that authority loose. When it takes place in a Title III context, the restriction on what is overheard from those incidental interceptions of people who the target calls is protected by minimization procedures. Just the same way when somebody calls a target—when you are targeting somebody overseas and they call an American, that is also protected by minimization procedures. Correct?

Mr. MCCONNELL. That is correct.

Senator WHITEHOUSE. The difference, as I see it, is that in the domestic surveillance context, the enforcement of those procedures, whether the agency actually obeys the rules that they are under, is not only enforced by the agency itself, but consistent, again, with the separation of powers principles of the United States, the court that issued the original warrant has some oversight authority over whether or not the minimization procedures in its order are complied with. Correct?

Mr. MCCONNELL. That is my understanding.

Senator WHITEHOUSE. That does not follow into the foreign targeting situation, and so if we were to make an equivalent role for the FISA Court, to me it would require the FISA Court to do two things: one, approve the minimization procedures themselves—which, frankly, they do every time they issue a warrant, because they are right in the order.

Mr. MCCONNELL. That is correct.

Senator WHITEHOUSE. And, two, have a role in making sure that the procedures are, in fact, complied with by the agencies. Would you have any objection to the FISA Court having that role in a general way?

Mr. MCCONNELL. You just introduced a level of complexity and uncertainty that I would say I would be happy to look at it. Now, what do I mean by that? In every case where there is Title III, in every case, a court has already agreed in advance that you are going to conduct this surveillance. And there are even—as I understand it, there are even some requirements for the Government to notify the party that you conducted surveillance against in a criminal situation.

In the context of foreign intelligence, the mission is entirely different. It is foreign intelligence, foreign threat to the country. So the way you described it, while it can sound reasonable, might it put the court in a position of having to decide in advance what we could do with regard to foreign surveillance. So I would say—

Senator WHITEHOUSE. No, that is not my intention either. My intention simply is to assure that if you got into a situation in which there was a renegade area in the intelligence community someplace in which they just simply were not complying with minimization—we have had unfortunate instances about the National Security Letters and the rules just were not complied with. It is helpful, I think, and it is salutary for the executive branch officials discharging a responsibility like that to know that a court can look in. And whether it is the Inspector General reporting to the court or whether there are some—but I do think that it is critical that there be a FISA Court role just as there would be for incidental intercepts on the U.S. side to oversee and make sure that the incidental intercepts are being minimized properly in the intelligence context.

Mr. MCCONNELL. Yes, sir, and when we discussed this before, the same answer. I am happy to sit down and take the language, look at it and have it examined, with some time—not like where we were before—so that we really understand what are the intended and the potentially unintended consequences, and so that we both satisfy ourselves that we are protecting Americans and we are not impacting our foreign intelligence mission. I would be happy to do that.

Senator WHITEHOUSE. Mr. Chairman, I think if we are thoughtful about going about this the way the Admiral has suggested, we will find that a lot of the disagreement and concern and anxiety and, in some cases, anger and frustration that emerged in the August stampede can be easily worked through, and we can get to a bill that makes a lot of sense for Americans and is consistent with the expectations that are longstanding under Title III.

Thank you very much.

Chairman LEAHY. Well, the Senator from Rhode Island is right, and one of the reasons for having these hearings now well in advance of the time when the sunset provision comes is so we can do that. Of course, many of us thought we had worked out that, and we were quite surprised when apparently at what many of us felt was the last moment, it seemed the administration had a different idea. The Chairman of the Senate Intelligence Committee has written a significant letter, and I don't know if that letter is classified or not, but I know the Senator from Rhode Island has seen it.

Senator Kyl.

Senator KYL. Thank you, Mr. Chairman.

Admiral, you have made the point, I think, very clear that the intelligence collection at issue here is vital to our national security and that Americans' rights are not being violated. But from a lot of the questions, I suspect to the average American this seems very complicated. And I would like to just have you explain two things for us using the most direct language you can in a non-classified context: to explain why this kind of collection is not suited to the usual court procedure for a criminal suspect, like we would see in a TV series, for example, and why it is not constitutionally necessary in any event.

Mr. MCCONNELL. Sir, the situation we find ourselves with is literally there are billions of transactions, and the targets of foreign surveillance are very dynamic and they change, and they could change modes of communication and so on. So for us to have the inherent flexibility that we need to be responsive and to collect the information we need to protect the country, being encumbered by a court process to extend due process rights to a foreigner, a terrorist located overseas, puts us in a situation where we can't be flexible, we can't keep up. We started this process last winter, and because of the wording in the old law, it was requiring us, because communications completely flipped from 1978 until today, whereby international communications were on a wire, fiber optics, and they happened to flow through the United States, then we were in a situation to do foreign target, foreign country, we had to stop and get a warrant.

It is so dynamic that we were losing ground. We had a level of capability. It was reviewed by the court. We started at that level.

And subsequent reviews—not because of the court, because of the wording in the law—we started reducing our capability. It was reduced in that review period about two-thirds.

I thought, OK, we just add more resource, we go faster, whatever. The issue is there is a finite number of linguists and analysts that speak the languages, understand the problems, so you are forced into a situation of pulling people off position to write probable cause standard warrant requests for a foreigner overseas. And as a practical matter, we are falling further and further behind.

So I felt a responsibility to identify that as an issue. The law captured it one way in the late 1970s. Technology changed, and we just need to recognize that and accommodate it to make it technology neutral. That is the sum and substance of what we are attempting to do.

I mentioned earlier that what I was after was three points: no warrant for a foreign terrorist located overseas; a way to compel and cause protection of the carriers that would assist us, because we can't do this without them; and then to require this community always, always, always, to get a warrant anytime it involves surveillance of a U.S. person.

And so those were the principles, and we are where we are with this law that was passed, and we are going to review it again. That is what I am going to try to maintain consistency with regard to our capability so we can indeed protect the country. And all the things that are suggested—there were seven bills exchanged back and forth. Some of them attempting to fix A, in fact, shut us down at B or C or D. And that is why I say happy to look at it, but we have got to examine it in the cold light of day.

Senator KYL. Never in the past—and, again, I hate to make it a matter of entertainment, but you see the spy movies and so on, when we send our spy abroad or James Bond is out looking to collect secrets. If you are abroad and you are collecting secrets against an enemy that is abroad, there has never been a requirement for a court warrant, has there?

Mr. MCCONNELL. No, sir.

Senator KYL. And it is arbitrary distinction, therefore, that in this particular case, just because a particular transaction happens to be routed through the United States but still involves foreigners, in terms of the reason for a change, there is no new reason for the change.

Mr. MCCONNELL. No, sir. The attempt was to take what was captured in 1978, which in my view was right, and make it relevant to 2007.

Senator KYL. And this is very important information in going after terrorists that we are fighting.

Mr. MCCONNELL. Sir, it is vital. If we don't have access to this, we are in most cases blind.

Senator KYL. And when you finally identify an American as somebody that we want to target, then the procedures, the usual due process procedures that we see, then they apply.

Mr. MCCONNELL. Yes, sir.

Senator KYL. Now, some have said, well, but if you find that you are beginning to focus in on somebody because he is making quite a few domestic calls, calls that you cannot know when you first

look at what he is doing where those calls are going, but it turns out that some of them start being made domestically, first of all, might that be important for us to know? And if so, why? And—well, let me ask that first.

Mr. MCCONNELL. It could be the most important call we would do in a long period of time because that may be activating a sleeper cell. So the only way we know that is when a targeted foreigner activates by calling in. So that is why it would be essential for us.

Senator KYL. And if you had some kind of arbitrary number and they said, well, you have to have a warrant if the person has made more than 15 calls into the United States or something, it would be pretty obvious. What they would do is simply make 16 calls to a pizza parlor or something and then make another call.

In other words, if we put statutory limitations—they are in statutes and, therefore, obviously are public—it could be possible for terrorists to get around the intent of what we are trying to accomplish here.

Mr. MCCONNELL. Yes, sir. That would take away our inherent flexibility. I would also highlight that in the eyes of the law, a U.S. person could be not only a human being, it could be a corporation. So if terrorists are ordering parts or scheduling travel or whatever, that may be the vital interest to us to track the terrorist, not intending that we are tracking a travel organization or an airline or whatever.

So the point you made is very, very important. It is the inherent flexibility to be responsive to the threat in a way that is useful, still respecting civil liberties by, if that person ever becomes a target, then you do a warranted process.

Senator KYL. In terms of fighting these particular Islamic terrorists who have both attacked us here and also attacked us abroad, there is sometimes a debate about what is more important—fighting in a place like Afghanistan or Iraq, or having good intelligence. I have always had the view that ultimately the best way to protect our homeland involves two things: denying these terrorists a sanctuary, a free place to operate, but also, and perhaps even more importantly, having absolutely the best intelligence so that we can understand what they are up to and, therefore, better protect the homeland.

How would you characterize the importance of this kind of intelligence gathering in this particular conflict?

Mr. MCCONNELL. Sir, it is essential, and I would go further to say the terrorist group that we are all talking about, al Qaeda, is very resilient and adaptive. We know their intent, and they are going through a process now to figure out how to recruit, train, and prepare an operative and get them back into the country to have attacks similar to 9/11 or something of that nature.

So the challenge for us becomes how do we see it, know it, understand it, and prevent it, and this process in large measure is how we do that.

Senator KYL. In time.

Mr. MCCONNELL. Yes, sir. In time.

Senator KYL. Thank you.

Chairman LEAHY. Admiral, are you aware of any time that this administration has asked for a change in the FISA law when it has not gotten it?

Mr. MCCONNELL. I think there was a request—yes, sir, last summer, I believe. Some of the members of this Committee introduced legislation that was passed on the House side, but I guess there was no agreement, so it did not pass.

Chairman LEAHY. But was that requested by the administration?

Mr. MCCONNELL. I don't know the origin of the source.

Chairman LEAHY. There were seven or eight during this administration. It seems we must have been answering some of their questions.

Mr. MCCONNELL. The language originated on the Hill last year, sir, I have just been advised. I was not playing, sir. I just didn't know.

Chairman LEAHY. OK. Now, you have referred to the use of minimization procedures, and those of us who have been here since the beginning of this law are aware of those. But under the Protect America Act, minimized communications are not destroyed. They are maintained in a data base. Is that not correct?

Mr. MCCONNELL. That is not correct. No, sir.

Chairman LEAHY. It is not.

Mr. MCCONNELL. If they are minimized, you would take them out of the data base. Minimization today is exactly as it was in 1978. That was the agreement, the process that was agreed to then.

Chairman LEAHY. So these minimized communications are not maintained in the data base?

Mr. MCCONNELL. No, sir. If it is in the data base and recognized, it would be expunged from the data base. Now, what you are making reference to is this is the fourth hearing on this subject since last Tuesday, and in there what I talked—in a previous hearing I talked about data that may be collected in a data base that you don't know it is there.

Chairman LEAHY. All right.

Mr. MCCONNELL. You wouldn't know it is there until you had a reason to go search it. So it could be there. It just—

Chairman LEAHY. Under the Protect America Act, the FISA Court has no role in the oversight of minimization, does it?

Mr. MCCONNELL. It does if there is—anytime it involves a warrant and a U.S. person, the Court would in its ruling have available to it in the context of minimization—

Chairman LEAHY. Are they shown the minimization procedures the Government uses?

Mr. MCCONNELL. I am sorry, sir?

Chairman LEAHY. Are they shown the minimization procedures—

Mr. MCCONNELL. Yes, sir, they are.

Chairman LEAHY. I will do a couple of followup questions on this for the record, and I hope you and your lawyers look at it very, very carefully. As I said, I am not trying to play "gotcha." And if there are answers in here where, upon reflection, you think they should have been different, you have plenty of time to do that.

Mr. MCCONNELL. I appreciate that, Mr. Chairman.

Chairman LEAHY. You have identified as one of your highest priorities giving the retroactive immunity—and we have touched on this, several of us have—to communication companies that may have broken the law in helping to carry out the Government's secret surveillance program after 9/11. As you may know, the State of Vermont, along with a number of other States, is seeking to investigate some telecommunication carriers for disclosing consumer information to the NSA in that program. There is a lawsuit, I believe in the Ninth Circuit, that would be dismissed if the carrier is granted immunity. That is why I asked the question about taking.

Now, this Committee has issued subpoenas, voted for by both Democrats and Republicans, seeking information on this. We have received no documents, no information about the legal justification for the warrantless surveillance program. We are in the dark about what the legal justification was, what communications took place between the administration and the communication companies to secure private sector cooperation for the program. For 2 years, we have been seeking the legal justification and the analysis and what the administration relied on to conduct the President's program of warrantless surveillance. We are, however, asked to pass laws to immunize everybody and to wipe out of court any cases. And basically we are asked to do that on a total "trust me" basis. We will not tell you what we did or what we based it on or why, but please pass a law saying that you have made a studied conclusion that everything we did was OK and thus immunize us. I am not sure if you were presented with something like that you would be too eager to accept that.

Do you have any objection from an operational or a national security perspective to having the Congress see these documents, legal documents on which this justification was based, on either a classified or unclassified basis?

Mr. MCCONNELL. Sir, that is a call the White House will have to make. My personal philosophy in how to conduct this business is oversight is a good thing; it keeps the system honest. And so engaging with the Congress and providing the appropriate level of information for the oversight process is what we should do.

Now, that said, there are going to be judgment calls about what is privileged or not, and there will be differences of opinion. The Constitution did say co-equal bodies, and a lot of this is at the constitutional level. So you are asking me if I can solve that. I cannot.

Chairman LEAHY. No. I am saying as DNI, just simply as DNI. Obviously, the judgment call is going to be made by the administration. But as DNI, do you have any objection to these legal memoranda being shared, these historical legal memoranda being shared with this Committee?

Mr. MCCONNELL. Sir, my history on this starts in January when I was nominated and February when I was confirmed. What I am trying to do in my role—

Chairman LEAHY. But, obviously, you have seen historical legal—

Mr. MCCONNELL. I have not. I have not. What I have attempted to do here is to take where we are today and put it wholly under the law and the FISA process for how we conduct our business. All of it. There is nothing extreme or—so anything that we do in the

nature of the business we are talking about would make it—I would be happy to—

Chairman LEAHY. But, Admiral, you are up here lobbying to have us wipe out these cases retroactively by legislation.

Mr. MCCONNELL. Sir, I would—

Chairman LEAHY. I mean, isn't this kind of asking us to buy a pig in a poke?

Mr. MCCONNELL. No, sir, it isn't. First of all, I would object to the word "lobbying." I am here because you invited me here. And I am testifying, not lobbying.

Chairman LEAHY. I am thinking of some of it during—I am going back to July and August in some of your meetings. You can call it whatever you want. You were advocating for retroactive legislation.

Mr. MCCONNELL. I have a responsibility as the leader of the Nation's intelligence community to make recommendations to this body and the administration about what it is we need to do our job, and that is how I saw my role, and that is what I hope to—in the final analysis, when it will be looked back on, that is what I was doing.

Chairman LEAHY. Are you conducting, if you want to answer this, under the PAA or otherwise, are you conducting physical searches of homes or businesses of Americans or Americans' mail without a warrant?

Mr. MCCONNELL. That would not be the business that I represent. If that situation were to take place, it would be the responsibility of the FBI, and they would do it with a warranted process.

Chairman LEAHY. But you are not?

Mr. MCCONNELL. No, I am not.

Chairman LEAHY. Senator Specter.

Senator SPECTER. Thank you, Mr. Chairman. Just a couple of questions, because we have another panel waiting to be heard.

When I questioned you on the first round, I brought up the issue of the targeting of U.S. persons overseas and noted that there is an Executive Order which requires the Attorney General to certify that there is probable cause. My own view is that there ought to be that determination made by the FISA court.

In response to a question of Senator Hatch, you said there are only about 50 to 55 of those a year, so it would not be a great administrative burden. Would you concur—or perhaps better stated, have any objection—to, in the next version of the statute, to give the FISA court the authority to authorize targeting U.S. persons overseas?

Mr. MCCONNELL. Sir, as I indicated earlier, I would have no personal objection. What we would have to do is look at the language to examine any potential unintended consequences. The difference would be the authority for the warrant going from the Attorney General into the FISA court. So that seems to me, on the face of it, to be a manageable situation.

There are reasons that we could go into in a closed session that it was set up the way it is, and I would be happy to share that with you. But let us examine that in closed session, make sure it does not have unintended consequences, and I would be happy to say, let's examine it.

Senator SPECTER. Are you saying that there are reasons vested in the Attorney General, the determination of probable cause, instead of the FISA court—and when probable cause is established, that is the traditional basis for the issuance of a warrant.

Mr. MCCONNELL. Yes, sir. Let me separate "U.S. citizen" from "U.S. person". In "U.S. citizen", it is easy. "U.S. person", it may present us a situation where we would just need to make you aware of the full range of potential impact.

Senator SPECTER. But it is "U.S. person" where you have to have a warrant for targeting in the United States.

Mr. MCCONNELL. That's correct, sir.

Senator SPECTER. So if the classification is "U.S. person", what difference would it make whether it's in the United States or outside the United States?

Mr. MCCONNELL. I was just trying to highlight, in my view, a U.S. citizen shouldn't be expected to give up their rights, regardless of where they're located. So it's a higher standard for "U.S. citizen" as opposed to "U.S. person".

A U.S. person can be a foreigner, or could even be a terrorist that was located in the United States, say a foreigner here, a green card. In the legal context, you could consider that person a U.S. person, even though they traveled back overseas. So I'm just trying to say there's an issue in there we need to examine.

Senator SPECTER. Well, I don't see the distinction between according the same degree of privacy to a U.S. person, whether they're in the United States or outside the United States, but we'll reserve judgment on that until we discuss it in closed session.

With respect to the approval of the FISA court on targeting people outside the United States, the objection has been made by you and the administration that there would be insufficient flexibility to require that going before the FISA court. But you acknowledge that the FISA court should review, at a minimum, their procedures. Correct?

Mr. MCCONNELL. Yes, sir. And you said "person". I would just highlight, make sure it's "foreign person located overseas". That's the part that they would—

Senator SPECTER. Foreign person located overseas.

Mr. MCCONNELL. Foreign person. Yes, sir.

Senator SPECTER. OK.

Now, you need the flexibility to do that without prior approval by the FISA court because of the numbers involved?

Mr. MCCONNELL. Yes, sir. It's a very dynamic situation.

Senator SPECTER. Dynamic. You mean large in numbers?

Mr. MCCONNELL. Large. Huge. Huge. Yes, sir.

Senator SPECTER. Dynamic meaning too many to do, you say?

Mr. MCCONNELL. Fast-changing. Yes, sir.

Senator SPECTER. Explain why that is.

Mr. MCCONNELL. The—

Senator SPECTER. Let me finish the question. Why you can't handle that administratively to submit those applications to the FISA court with a statement of probable cause.

Mr. MCCONNELL. Well, first of all, it's extending the probable cause standard and Fourth Amendment protection to a foreigner overseas. So my argument would be, to maintain the flexibility of

our community to do our mission, why would you insert that as a standard because it's an additional burden on the community to be flexible now?

Senator SPECTER. Well, it may be a burden, but that's not the determinant as to whether you ought to have the burden. The question is whether the burden is unreasonable and precludes you from doing your job. Is that what you're saying?

Mr. MCCONNELL. Yes, sir. It is unreasonable on the face of it and it precludes us from being effective in our job.

Senator SPECTER. OK. Now, the question is why? Just as a result of the sheer numbers?

Mr. MCCONNELL. Numbers and the dynamic nature of it. Most of our conversation today—

Senator SPECTER. That's the second time you've used the word "dynamic". Tell me what you mean by that.

Mr. MCCONNELL. Fast-paced, rapidly changing.

Senator SPECTER. OK.

Mr. MCCONNELL. And most of our discussions have been around terrorists. That's a reasonable number of people. But the foreign intelligence mission of the community is foreign, so by definition it's anything that is not American. When we have taken great pains in a number of cases to prioritize who we target and so on, we inevitably get it wrong. In the previous administration, we did a tiering mechanism, like 1 through 5. Five was absolute targets, got to cover them, got to be very exhaustive in our coverage.

As it turned out, where U.S. forces were asked to engage or in some way be committed, it was almost all in the tiered areas that we weren't covering. Examples include Haiti, Somalia, and even as far back as Panama. Those situations that pop up in which you have to be responsive and dynamic to respond to so you understand who the threats are, how they're changing, what are the intentions, what are the weapons systems, how might they engage, what might cause them to back down. All that is a very dynamic issue.

Senator SPECTER. So you're saying you have to respond immediately?

Mr. MCCONNELL. Yes, sir.

Senator SPECTER. Have you gone back to the FISA court to go through the procedures which you're now using in targeting foreign persons overseas?

Mr. MCCONNELL. Yes, sir. We submitted all the procedures to the court and they're reviewing them now.

Senator SPECTER. They're reviewing them?

Mr. MCCONNELL. Yes, sir.

Senator SPECTER. Would it be too burdensome to ask you to submit those procedures to the court every three months?

Mr. MCCONNELL. They wouldn't change, but that would not be a great burden. No, sir.

Senator SPECTER. OK.

Mr. MCCONNELL. The only thing I want to highlight is, if I'm in a position where the court has to rule on something before I can conduct a mission, we could never turn fast enough to allow us the flexibility.

Senator SPECTER. My suggestion would not be to deal with specific warrants where you'd have to go back, but only the procedures.

Mr. MCCONNELL. Yes, sir.

Senator SPECTER. But if you did it every three months, wouldn't it be reasonable, on the reapplication, to show the court what you have accomplished so that they could then consider the value of the program in deciding whether the procedures are sound?

Mr. MCCONNELL. Sir, I would object to that because in my view it would now start to insert into the process an evaluation by the court for which it is not trained or prepared with in regard to the effectiveness of the foreign intelligence mission. Let me use a couple of examples.

Senator SPECTER. Well, now, wait a minute. Are they any less prepared for that than they are for determining the importance on targeting a U.S. person in the United States?

Mr. MCCONNELL. The purpose, in my view, of targeting a U.S. person in the United States is to ensure that we have adequate protections for a person in the United States. They will examine—first of all, the numbers are small, very small. They would have the facts of the situation. They could make a judgment and they could do enough research to make an informed judgment. If you're talking about thousands, tens of thousands, or hundreds of thousands of things that are transpiring in a foreign context, my view is that they just couldn't keep up with that process. There are 11 judges. One sits at a time.

This community is made up of tens of thousands of people that engage in a very dynamic process, issuing lots of reports, lots of coordination, and lots of cross-queuing. So something that seems relatively innocuous on the face of it might turn out to be the most important thing we're chasing.

Example. Movement of nuclear material on a foreign flagship of convenience that is moving from the Pacific into the Indian Ocean. We may not even know that ship is under way, but at some moment there is some clue and we have got to be very responsive in how we would try to track back, where did it originate, what might it have on board, where is it going, who are the players, and so on.

That's just the situation we find ourselves in on a regular basis. That's just one tiny segment of the community. So that's what I mean by very dynamic and very interactive. We're trying to solve a foreign intelligence problem that someone in the administration has a need for, tracking nuclear material, preventing weapons of mass destruction, negotiating with a country that might receive it, whatever. You can go on and on and on.

Senator SPECTER. I get your point, Director McConnell. I am over time, but this is important and I want to finish it.

Mr. MCCONNELL. Yes, sir.

Senator SPECTER. I get your point on the dynamism of being able to act without getting court approval. But I'm on a very different point. I'm on the point of going back for renewal, say, in 3 months as to procedures, and at that time saying to the court, we want to continue this under these procedures, and this is what we've accomplished.

Because without telling you you can't do it, but we want to evaluate it, you are reaching some U.S. persons overseas, and we have elaborate minimization, it seems to me that there is a good basis for having the court take a look at what you've done to see the intrusiveness, even though there are a lot of foreign people involved, but there are some U.S. people involved, as to whether it's worth the candle.

Mr. MCCONNELL. Sir, the reason I would object to it is, at the 99.99 percent level, it's totally foreign. So by having the court make that judgment, you are introducing a level of ambiguity and uncertainty that I don't know how it would come out. So now let's go back to the U.S. persons situation. In that case, if the court chooses to look at it, they've issued a warrant and post facto they want to review, or as was suggested by Senator Whitehouse, they look at minimization after the fact. That's more of a manageable problem.

But to have the court in a position of saying what you collected is or is not of sufficient intelligence value, in my view that's not the appropriate role for the court. My worry is a level of uncertainty and ambiguity that I don't know how it will come out. We do the mission for foreign intelligence. There are oversight committees on the Hill that look at that, can evaluate it in any cross-cut or any dimension, and we're responsive to the administration, who has given these targets for foreign intelligence collection purposes.

Senator SPECTER. Well, I'm not satisfied with this answer, but we have to move on. You and I will talk about this further. Thank you.

Chairman LEAHY. I think it's a good issue. I also will follow-up. I think Senator Specter has raised a very valid question and we should talk about that more, certainly before we get to the time we have to reauthorize any part of this Act.

Admiral, I know you are an extraordinarily busy man and I appreciate you being here. We will have some follow-up questions. Some may have to be answered in classified form. Of course, we have provisions to handle that, as you know. You should also feel free, on some of the questions I may have, if you have a question on it, just call me.

Mr. MCCONNELL. All right, sir. Will do. Thank you.

Chairman LEAHY. I'm easily reachable.

So now, thank you very much. We'll set up for the next panel.

Senator Feingold has offered to preside in my absence, and I appreciate that. He is also a member of the Senate Intelligence Committee, which will make it twice as helpful.

Senator FEINGOLD. We will now turn to the second panel of witnesses, if they would come forward, please.

Will the witnesses please come to the witness table and stand to be sworn in? Would you all please raise your right hand to be sworn?

[Whereupon, the witnesses were duly sworn.]

Senator FEINGOLD. Thank you. You may be seated.

I want to welcome all of you, and thank you for being here with us today, and for your great patience while the committee questioned Director McConnell.

I ask that you each limit your opening remarks to 5 minutes, as we do have a fair amount to go through. Of course, your full written statements will be included in the record.

Our first panel begins with James Baker. Mr. Baker is a lecturer at Harvard Law School, currently on leave from the Justice Department. Until January of 2007, he served as the head of the Office of Intelligence Policy and Review at the Department of Justice, which is the office that represents the government before the Foreign Intelligence Surveillance Court.

In 2006, Mr. Baker received the George H.W. Bush Award for Excellence and Counterterrorism, the CIA's highest award for counterterrorism achievements.

Mr. Baker, you are, of course, welcome. Thank you for being here today. You may proceed.

STATEMENT OF JAMES A. BAKER, LECTURER ON LAW, HARVARD LAW SCHOOL, FORMERLY COUNSEL FOR INTELLIGENCE POLICY, DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. BAKER. Mr. Chairman, thank you very much, and members of the committee. Thank you for the opportunity to appear here before you today to discuss possible changes to FISA and the Protect America Act.

I would just comment on my background, that in addition to what you mentioned, Mr. Chairman, I have prepared, reviewed, or supervised the preparation of thousands of FISA applications over the time period that you're talking about.

The Department of Justice has specifically approved my appearing here before the committee today, but let me emphasize that I am appearing here strictly in my personal capacity and that the views that I express do not necessarily reflect those of the Department or the administration.

In the short time that I have, I'd just like to focus on a couple of brief points, Mr. Chairman. First of all, FISA, as originally enacted by Congress in 1978 and as amended up until the Protect America Act in August of this year, was extremely productive over the years. It permitted robust collection of foreign intelligence information, including actionable intelligence information, which means that the Intelligence Committee could take action on it to thwart the plans and activities of foreign adversaries, including terrorist groups. As a result, in my opinion FISA has proven very valuable during wartime.

We did this in part by making robust use of FISA's emergency provisions. I am happy to discuss those provisions and the procedures with you in response to questions, but I just would note that it may take some time to do that in order to give a proper description of how the system actually worked.

In addition, FISA also permits us to disseminate foreign intelligence information appropriately within the U.S. Government and to our foreign partners. It allows us to use information acquired as evidence from a FISA collection in criminal trials, with the approval of the Attorney General.

In addition, everyone within the system had the comfort of knowing that their actions were lawful and that they would not be sub-

ject to lawsuits or criminal prosecution as a result of an action that they were taking in accordance with an act of Congress and a Federal court order.

Let me also state that it seems to me that there's a bit of a paradox here in the discussion that we're having because the calls for FISA to be amended—the original FISA to be amended—came ultimately from the success of FISA itself.

Because FISA had enabled the collection of vital, timely intelligence, including information about the activities of overseas terrorists, the intelligence community came to regard FISA as a critically important collection platform and it increasingly turned to FISA to obtain important foreign intelligence.

FISA also expanded the understanding by other intelligence community elements of the value of certain types of collection. Growth in the targeting of foreign operatives over time resulted in the desire to change the law that we are discussing today.

What I would suggest is, before you decide to renew or amend FISA or the Protect America Act, or make other changes to FISA, I would recommend that you ask the intelligence community for a full assessment of the value of FISA as originally enacted, or at least as enacted prior to August of this year.

Let me just make a few brief comments about the scope of the original FISA. No means of collection were barred by the 1978 statute. In other words, all modern forms of communication were subject to collection under FISA.

My written statement discusses some of the questions that have arisen regarding the state of technology in 1978, what Congress understood about that technology, and what it intended to cover when it enacted FISA, and what the law actually says. For the sake of brevity I will not repeat those here, but I will just say that they are complex questions that require additional research to answer authoritatively.

At the end of the day, though, the real questions, it seems to me, are not regarding whether, or how, to modernize FISA and are not technological in nature. The real question at the end of the day is whether the government's collection activities comport with the Fourth Amendment.

The answer to that question will depend on many factors, including, but not limited to, the following. First of all, what is the identity and the location of the person or persons whose communications are collected and reviewed?

For example, where is the target, U.S. or abroad? Who is the target, a U.S. person or a non-U.S. person? Whose communications are intercepted in addition? We've talked about that before. The committee talked about that before with respect to incidental communications, but it's broader than that as well. What is the identity of these people whose communications are being collected?

The next thing is, with what degree of confidence can you answer the questions that I have just posed? Do you really know where these people are? Do you really know who they are?

In addition to those questions, there is another set that have to do, it seems to me, with the collection procedures that are in place. So, for example, who is the decisionmaker? That is, who is making

the decision about foreign intelligence collection before it begins? Someone from the executive branch, a Federal judge, for example?

What level of predication is required—that is, how much paperwork and explanation is necessary to justify collection—and what standard of review should apply? Should it be probable cause, something lower, no standard at all? What should it be?

Further, how particular should the approvals be? Should they be specific with respect to a particular phone number? Can they be more programmatic? How exactly should it work? In addition, what are the standards for acquiring, retaining, and disseminating foreign intelligence information? These are the minimization procedures you've just discussed at length. Further, how long can the collection run without being reviewed?

The lower the level of approval and the lower the level of factual predication and the less specific the authorizations need to be, obviously the more quickly and more easily the intelligence community can start collection and sustain a greater volume of collection. I think that is what is meant by when someone says we need to achieve greater speed and agility in foreign intelligence collection.

Again, the Fourth Amendment lies at the foundation of all these questions. When the government—

Senator FEINGOLD. Mr. Baker, I'm going to have to ask you to conclude.

Mr. BAKER. I'll sum up very quickly. Let me just focus on this. There are Fourth Amendment interests at issue. The Fourth Amendment is implicated during the following situations: when the government targets U.S. persons or people in the United States, when it acquires, listens to, or stores and later examines, a communication to which a United States person is a party, or when it intercepts and scans the content of such a communication in order to determine who it is to, from, or about.

Let me just say that when I say the Fourth Amendment is implicated, I do not necessarily mean that a warrant is required in all those situations, but the collection has to be reasonable when you're collecting information about people who are protected by the Constitution.

Mr. Chairman, thank you for your time.

Senator FEINGOLD. Thank you. I regret our time limitations and appreciate your testimony.

[The prepared statement of Mr. Baker appears in the appendix.]

Senator FEINGOLD. Our next witness will be James Dempsey. Mr. Dempsey is no stranger to testifying before Congress. We are pleased to have him with us today. He is currently the Policy Director at the Center for Democracy and Technology, where he has been on staff since 1997.

Prior to joining CDT, Mr. Dempsey was Deputy Director of the Center for National Security Studies, and before that Mr. Dempsey was Assistant Counsel to the House Judiciary Committee on Civil and Constitutional Rights, where he concentrated on oversight of the FBI, privacy, civil liberties, national security, and constitutional rights. He is also the author of a number of articles on privacy and Internet policy.

Thank you for being here, sir, and you may proceed.

STATEMENT OF JAMES X. DEMPSEY, POLICY DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY, SAN FRANCISCO, CALIFORNIA

Mr. DEMPSEY. Senator Feingold, Senator Specter, Senator Whitehouse, good afternoon. Thank you for the opportunity to testify at this hearing.

As the committee well knows, the issue before Congress has nothing to do with terrorism suspects overseas talking to other people overseas. The debate for the past year has been about the communications between people in the U.S. and people overseas.

Here is the dilemma. The National Security Agency needs speed and agility when targeting persons overseas. It should not be required—not be required—to get individualized orders when targeting non-U.S. persons abroad. Many of NSA's targets overseas will communicate only with other foreigners, never affecting the rights of Americans.

In addition, NSA can often not tell in real time who a foreigner overseas is communicating with, and obviously it can certainly not predict in advance whether a targeted person overseas will communicate with an American or not sometime in the course of a coverage.

We recognize these concerns. However, it is also certain that some of the persons of interest to NSA overseas will communicate with people in the U.S. Some percentage of NSA's activities targeted at people overseas will result in the acquisition of communications to and from American citizens, and those will be retained, analyzed, and in some cases, disseminated.

So how can we give the government the flexibility, the speed, and agility it needs while protecting the rights of Americans whose communications are being intercepted and disseminated? Now, at this hearing so far I've heard a lot of progress being made and I've heard the outlines of an approach that is better than the approach in the Protect America Act along the following lines.

First, use plain English, not the ambiguous and confusing language found in the Protect America Act. The DNI said he can't even remember now why the word "concerning" was used in the legislation. The issue at stake concerns—and here is where I would focus—the government's authority to acquire communications to or from non-U.S. persons reasonably believed to be outside the United States when those communications are acquired, in real-time or in storage, with the assistance of a communications service provider. Say it that way, plain English. That would clear up a lot of the concerns about physical searches, mail openings, et cetera. The DNI, I think, agreed that better language is needed.

Second, is to focus, as the DNI says, on the rights of Americans regardless of geography, require a particularized court order when the government is targeting a U.S. person regardless of where the U.S. person is. Again, I heard the DNI say, at least in principle, that he accepted that proposition.

Third, establish a procedure for the FISA court to review and approve in advance the procedures for ensuring that the persons being targeted abroad are reasonably likely to be non-U.S. persons outside the United States. Now, it should be a real judicial review

and not the clearly erroneous standard that's in the PPA, a genuinely effective standard.

By prior review—and I think this is where Senator Specter and the Director of National Intelligence had a little disconnect—we don't mean a prior individualized warrant. We would say, though, that the court should look at the procedures for how, generally speaking, the targeting is done and also should review in advance the minimization procedures.

Again, the DNI said that he would submit the minimization procedures to the court for review, not in a way that would interrupt their individualized targeting, but in a way that would protect the rights of Americans. Bringing the surveillance under a court order has numerous advantages.

It would make the surveillance more likely to be found constitutional. It would provide companies with the greater certainty that they would get from a court order compelling their cooperation rather than just a letter from the Attorney General, and it would give the court ongoing jurisdiction to supervise how the minimization rules are being applied.

On that point, the fourth element that I heard some beginning of agreement on, the DNI said they have a procedure at the analysis and dissemination stage—not at the collection stage, but at the analysis and dissemination stage they have a procedure for determining who is a U.S. person.

That should be noted, recorded, and reported to the court, and at a certain point the court will decide that the focus of this investigation or the focus of this activity has now implicated the rights of an American to the extent that an individualized order may be required.

Finally, a balanced solution would address exclusivity and immunity. The issue of future exclusivity must be addressed and resolved first, since it has to be made clear that service providers will not get an ongoing series of free passes for violating the statute.

This approach addresses all of the concerns of the administration, while still providing the court approval and ongoing supervision that were the cornerstones of FISA. The DNI talked about the importance of flexibility. What I heard today, urging from the questioning, was a system of supervised flexibility, and that is where I think we should go. Thank you.

Senator FEINGOLD. Thank you for your useful testimony, Mr. Dempsey.

[The prepared statement of Mr. Dempsey appears in the appendix.]

Senator FEINGOLD. Our next witness is Bryan Cunningham. Mr. Cunningham is an information, security, and privacy lawyer and a principal at the law firm of Morgan & Cunningham in Denver, Colorado. Mr. Cunningham has held senior positions in both the Bush and Clinton administrations. He served for 2 years as Deputy Legal Advisor to then-National Security Advisor Condoleezza Rice.

Mr. Cunningham, please proceed.

STATEMENT OF BRYAN CUNNINGHAM, PRINCIPAL, MORGAN & CUNNINGHAM, LLC, GREENWOOD VILLAGE, COLORADO

Mr. CUNNINGHAM. Thank you, Mr. Chairman, Senator Specter, members of the committee, and thank you for the opportunity to again address the committee on this important issue.

Just one other background bio note I would make, is that I served for 6 years under President Clinton and 2 years under President Bush. Shortly after the disclosure of the terrorist surveillance program, a Democratic colleague and I published an op-ed piece in which we suggested that the eavesdropping debate we should be having would have three touchstone elements: 1) it would maintain the balance between civil liberties and national security that was enshrined in the original 1978 statute, but in ways that caught up with technological change, which in our view had clearly made the statute unworkable; 2) in doing so it would ensure that, while perhaps the methods would not be the same, the same civil liberties interests would be protected; 3) specifically it would provide a meaningful role for the courts in that process. I believe, Mr. Chairman, that the Protect America Act has taken significant steps in that direction, although it could use improvement. I commend the committee for continuing to carry on a sober debate such as recommended.

Just a little bit of recap of history from my point of view. The presidents of both political parties since at least 1946 had conducted significant programs of warrantless electronic surveillance for foreign intelligence purposes, including in this country.

As you know better than I, in the late 1970s following revelations about what I would call "true domestic spying" as opposed to what in my view is going on today, which is foreign intelligence collection, the Congress and the administrations of two parties reached a very good, as the Director said, balance between those legitimate interests.

The means they chose to effect that balance between privacy and civil liberties on the one hand and national security, perhaps were sensible and enforceable at the time, but I think now, because of changes in technology that have been publicly discussed, that balance needs to be struck in a new way. I think the Protect America Act starts to do that.

But I think we need to be clear about what we're doing in modernizing the Foreign Intelligence Surveillance Act. My understanding of the original statute was that it attempted to strike the balance principally by requiring, as has been said here today, a warrant for targeted surveillance of Americans inside the United States and no warrant for targeted surveillance of foreigners overseas.

Even in 1978, it was well understood, as it has been by all Congresses and presidents since, that in the course of targeting non-U.S. persons overseas there would be significant amounts of what is called in the law "incidental collection", that is, a foreigner talks to someone in the United States. Some of that is completely innocent, not of foreign intelligence value, gets minimized. Some of it is of foreign intelligence value and gets treated in a protective way, but can be shared around the community.

If we want to maintain that same bargain if you will, that same balance that was struck then and has been carried out over the last three decades under executive orders for collection targeted against persons overseas, I think we need to recognize that there will be this significant amount of incidental collection.

And when opponents of the Protect America Act talk about millions and billions of new collection activities against Americans, I can only guess that what they mean is that because we've removed the FISA restriction against collection inside the United States when targeted against foreigners overseas, the volume is simply going to go up by virtue of that.

If that is the objection, that's a point that we should recognize and debate. But we should be straightforward about it, that if we intend to now have courts regulate that incidental collection, we are now rewriting the bargain that was reached in 1978 and we're doing that during war time. Now, there may be legitimate ways to do that, but I think we need to recognize that that's what we're doing.

Now, I said the Protect America Act took significant steps in the right direction, and I believe that. I also believe we need a more proactive, earlier role for the Foreign Intelligence Surveillance Court in the process of approving procedures. I think it needs to be clear that they have access to more data, although I don't believe that court to be shy about asking for data when it needs it.

I think we should work to eliminate ambiguous terms and better define the terms that are in the statute, including specifically the issue of "concerning," as was discussed by the Director, and Senator Feingold, in your questions, and others', and also we do need to, I think, do something about protecting better the service providers who carry out lawful instructions by the government, and also to recognize that it is career civil servants who are carrying out these procedures, not politically elected officials, and we ought to make sure that we fully support them.

Finally, I would just say that I believe that there's technology that's available today that can solve many of the problems we're discussing here, including minimization, retention, collection, and use of information. Thank you.

Senator FEINGOLD. Thank you so much, Mr. Cunningham.

[The prepared statement of Mr. Cunningham appears in the appendix.]

Senator FEINGOLD. Our last witness will be Suzanne Spaulding. Ms. Spaulding's expertise on national security issues comes from 20 years of experience in Congress and the executive branch. She has worked on both the House and Senate Intelligence Committees and has served as Legislative Director and Senior Counsel to Senator Specter, the Ranking Member of the committee.

She has served as the Executive Director of two different congressionally mandated commissions focused on terrorism and weapons of mass destruction, and has worked at the CIA. She is currently a principal at Bingham Consulting Group, and the immediate past chair of the American Bar Association's Standing Committee on Law and National Security.

Senator SPECTER. Mr. Chairman, might I add—

Senator FEINGOLD. Absolutely.

Senator SPECTER.—a note about her outstanding service on my staff and on the Commission on Weapons of Mass Destruction where I served as vice chairman.

Ms. SPAULDING. Thank you, sir.

Chairman LEAHY. We're lucky to have her here.

Senator FEINGOLD. I agree. You may proceed.

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

Ms. SPAULDING. Thank you very much. Thank you, Senator Feingold, thank you Ranking Member Specter, members of the committee. I very much appreciate this opportunity to testify on changes to the Foreign Intelligence Surveillance Act, or FISA.

In the 20 years that I spent working on efforts to combat terrorism, starting in the early 1980's working with Senator Arlen Specter, I developed a strong sense of the seriousness of the national security challenges that we face and a deep respect for the men and women in our national security agencies who work so hard to keep us safe.

We all agree that we owe it to those professionals to ensure that they have the tools they need to do their job, tools that reflect the ways in which advances in technology have changed both the nature of the threat and our capacity to meet it.

They also deserve to have clear guidance on just what it is that we want them to do on our behalf, and how we want them to do it. Unfortunately, the newly enacted changes to FISA do not provide clear guidance and instead appear to provide potentially very broad authority with inadequate safeguards.

I will highlight just a few key concerns in this brief statement. First, avoid changing definitions, particularly if something as fundamental as electronic surveillance. Because Section 105(a) defines out of FISA the acquisition of any communication when it's directed against someone reasonably believed to be outside the United States, it removes any statutory protection that FISA might otherwise afford Americans whose communications might fall in this category.

This means there is no statutory minimization requirement, no court review of procedures, no reporting requirement. Any executive orders, directives, or other internal policies that might continue to apply can be changed unilaterally by the executive branch.

Keep in mind that Section 105(b), which does require some minimization in reporting, is an optional process that the Attorney General and the DNI may use if they want to compel the assistance of a third party. If they can intercept the communication without any assistance of a third party or don't need to compel that assistance, they do not need to use those procedures in 105(b).

Second, the words "notwithstanding any other law", which is how the new Section 105(b) begins, should always raise a red flag. These words mean that all the laws that regulate collection of intelligence inside the United States no long apply to activities under 105(b).

Those activities are potentially extremely far-reaching. Section 105(b) appears to provide statutory authorization for the government to gather information on any kind of communication inside

the United States from U.S. citizens, so long as it is about someone who happens to be outside the United States at the time.

It would appear to include intercepting U.S. mail between U.S. persons and the physical search of a computer for stored e-mails without regard to the physical search provisions in FISA. None of this intelligence collection has to be related in any way to terrorism. It applies to "any foreign intelligence", a very broad term.

The Protect Act does require minimization procedures under 105(b), but only the relatively permissive procedures that currently apply when a FISA judge has approved an application against a foreign power or an agent of a foreign power. In the case of AG-authorized surveillance under 105(b), what should apply are far more stringent procedures that currently apply when the Attorney General unilaterally authorizes surveillance under existing Section 102 of FISA.

Changes to FISA should be the narrowest possible to remove whatever impediment has arisen to using FISA. My phone company always seems to be able to determine where I am when I use my cell phone. They charge me a lot more when I use it overseas. Technology experts, FISA judges, current and former, can provide insights into what the government and communications providers can and can't do, as well as what safeguards are most important to prevent abuse. This provides a basis for a legal regime that is much more narrowly focused, with precise procedures and safeguards to govern surveillance that involves persons inside the United States

In addition, the role of FISA judges should not be minimized. As Supreme Court Justice Powell wrote in the Keith case, "The Fourth Amendment does not contemplate the executive officers of the government as neutral and disinterested magistrates." Finally, Congress should seek a stronger commitment from the administration that it will actually abide by the law.

[The prepared statement of Ms. Spaulding appears in the appendix.]

Senator FEINGOLD. Thank you very much, Ms. Spaulding. Thank you all.

We will do 5-minute rounds, which I will now begin.

Mr. Baker and Ms. Spaulding, as we have already demonstrated, you both have a great deal of experience in the intelligence community. Why is it advantageous for intelligence professionals to have clarity and certainty in the laws that govern their activities, particularly when those activities affect the rights of Americans?

Mr. Baker.

Mr. BAKER. Well, because, as the DNI explained, what they do on a daily basis is fast-moving, it's dynamic, it's difficult. You're up against a very difficult target. The system is populated with folks who are not lawyers. They can seek legal advice, but they are generally not lawyers, so you need to have clear rules of the road that they can turn to when they do have a question. First of all, that they can understand and that they can turn to when they have a question, and then understand them.

Have them be in plain English, as Mr. Dempsey suggested. I mean, that's always a good idea. So the danger is that folks under pressure, acting quickly with limited time, will confuse what is set

forth in the standard, will be too aggressive, or the other danger is, they won't be aggressive enough. They won't go and do what it is that they should do. So you have both of those things. That's why you need clarity.

Senator FEINGOLD. Thank you.

Ms. Spaulding.

Ms. SPAULDING. I think that's exactly right. In fact, it was one of the issues that the National Commission on Terrorism, in 2000, looked very carefully at. It looked very carefully at the implementation of FISA and other authorities that the government had to pursue international terrorism, and reached the same conclusion, that there was a real national security cost in not having very clear guidance and clear guidelines, in large part because oftentimes then officials would not exercise the full scope of their authority, fearing that they would not know where that line was and they would step over it. But there are national security costs.

Senator FEINGOLD. Could you give a couple of examples of how that would happen?

Ms. SPAULDING. Well, I know one of the contexts in which this arose was in looking at the investigation authorities. It was a particular problem for the FBI in the counterintelligence and foreign intelligence context, as well as in the provisions for criminal investigations, where there were several attempts to issue clearer guidance to officers in the field because it was not clear to them exactly where the lines were in terms of what they could and couldn't do at the various stages of investigation. What we found was, there were many, many instances in which they thought the line was short of where it was and they were not stepping up and doing things that the law actually allowed them to do.

Senator FEINGOLD. Thank you.

Mr. Dempsey, the Protect America Act will clearly result in the warrantless interceptions of the communications of Americans with individuals overseas. What are the Fourth Amendment rights of the Americans whose communications are intercepted under the Protect America Act, and is the Protect America Act unconstitutional?

Mr. DEMPSEY. Well, I think it's fair to say that the Protect America Act is of dubious constitutionality I think in the national security arena, we cannot afford legislation or authorities that are of dubious constitutionality. We want the kind of certainty, we want to not have to make every case into a potential litigation or a potential court challenge.

There is no doubt that an American in the United States talking to somebody overseas has Fourth Amendment rights. You have a reasonable expectation of privacy in your phone calls, and that is regardless of whether it is a domestic phone call or a domestic-to-foreign call.

What I think the issue here is, how can we protect that Fourth Amendment right of the American, that privacy interest of the American, without going the whole route of a particularized, individualized, probable cause-based order when the intelligence agencies are targeting a non—U.S. person overseas? I don't think that the Protect America Act comes close to striking that balance.

Senator FEINGOLD. Thank you for that answer.

Ms. Spaulding, what message would it send if Congress were to grant retroactive immunity to private entities that allegedly were involved in the President's warrantless wiretapping program?

Ms. SPAULDING. Senator, I think it would send a terrible message, both to the American public and to private companies that might be asked in the future to help their government. I think it would send a loud and clear message that we are not serious about respect for the rule of law, and I think that would be very damaging.

In this area particularly there is not the kind of transparency even that you have in the criminal context where the collection of information will ultimately be challenged if it is to be introduced into court, for example, in this area where secrecy is so imperative, it is equally imperative that we have these safeguards in place and the telecommunication providers become our last line of defense against abuse by the government. Granting retroactive immunity, I think, would send the wrong signal about how corporations should react when they're asking to do something. It's not burdensome for them to ask the government to assure them that what they're being asked to do is lawful. That's all the law requires.

Senator FEINGOLD. Thank you very much.

Senator Specter.

Senator SPECTER. Thank you, Mr. Chairman.

Ms. Spaulding, you have testified about the changeability of the executive order. Would you favor a statutory provision which would require the FISA court to review the targeting on probable cause for issuance of a warrant against a U.S. person overseas?

Ms. SPAULDING. Senator, I certainly think there is value in putting the requirements that you want the government to follow in the statute. To the extent that that is currently a requirement in the executive order and the executive branch is following that and it has not presented any national security problems, I think it would be very wise to put it into statute.

Senator SPECTER. So you would rely on the Attorney General, contrasted with putting it to the FISA court, to determine probable cause, and therefore a warrant?

Ms. SPAULDING. I'm sorry. No. Right. Your question was rather than simply requiring the Attorney General, should we impose the FISA court. Again, it seems to me that there is an important role for the FISA court in protecting the Fourth Amendment rights of U.S. citizens. Clearly, we rely upon them to do that inside the United States.

Senator SPECTER. Is that a "yes" answer?

Ms. SPAULDING. I think it is a "yes" answer. Yes, Senator. The Fourth Amendment continues to protect Americans when they are overseas.

Senator SPECTER. Would you take on a little staff assignment here and give us the language you'd like to see on minimization, and also to protect, without ambiguity, a U.S. person overseas for having collateral collection of private matters while in the United States?

Ms. SPAULDING. Yes, Senator, I certainly will.

Senator SPECTER. OK.

Ms. SPAULDING. Always happy to be your staffer.

Senator SPECTER. Thank you. There will be some supplemental assignments, Ms. Spaulding.

[Laughter.]

Mr. Baker, you were quoted in The Hill today as saying that "in no kidding situations the FISA court can act very fast, on a very prompt basis." That may undercut what Director McConnell has talked about, the dynamics which require executive action without court intervention.

Do you see any way, based on the extensive experience you've had with the Federal Government, where there could be more FISA court involvement on targeting people overseas?

Mr. BAKER. Absolutely. I think there is a way to work the FISA court into the system for dealing with folks overseas, targets overseas, and at the same time not cripple the ability of the intelligence community.

Senator SPECTER. How would you do it?

Mr. BAKER. Well, it's complicated. I mean, there are a number of ideas that have been set forth today. For example, one thing could be to have the Attorney General make an application to the FISA court that is not talking about individualized, specific warrants, but that would be targeting non-U.S. persons overseas, and have the FISA court review the targeting decision as a general matter, review the means of collection.

Senator SPECTER. Let me ask you, because I have got less than 2 minutes left, to do a little drafting as to how you would suggest we get the FISA court more deeply involved.

Mr. BAKER. I am also happy to take assignments. Yes, sir.

Senator SPECTER. OK. Thank you.

Mr. Dempsey—and I'm going to ask you the same question, Mr. Cunningham—on the issue of having the FISA court evaluate the success of the targeting overseas without judicial intervention in advance, do you agree with my thought, Senator, that it's relevant to know how successful the administration has been, the Director of National Intelligence has been, in collecting valuable information without any judicial supervision, in evaluating the adequacy of the procedures employed by NSA?

Mr. DEMPSEY. Well, I think what you were talking about was in a way a return on service, which is, we've given you this authority, and it may be a blanket authority to target at will, so to speak, with flexibility and speed, persons overseas. But then there should be a report back to the court on, how is it going? Are you primarily, in fact, collecting persons overseas? We know that it is probably going to be rare that they are talking to people in the U.S., but how often after analysis did you conclude—

Senator SPECTER. Is that a "yes" or a "no" answer?

Mr. DEMPSEY. That's a "yes". That is a "yes".

Senator SPECTER. Mr. Cunningham, do you think there ought to be some special reporting back to the court where there's information gathered from people in the United States, even though the targeting might be outside the United States?

Mr. CUNNINGHAM. Well, Senator, I think there are two aspects to that.

Senator SPECTER. Take your time, because I will not ask any more questions. My red light is on.

Mr. CUNNINGHAM. I think there are two aspects to the answer. One, is the constitutional, legal one. As you know, courts have almost never been involved in supervising the collection of foreign intelligence overseas, so as a constitutional matter I think there is a question as to whether or not we want to initiate that. However, as a policy matter, as a good government matter, I do think that there should be, as I suggested in my opening statement, a more robust role for the court in overseeing the process.

But where I would disagree with you, respectfully, Senator, is I don't think the court can be in a position independently to evaluate the foreign intelligence value of the information. Was it helpful to conducting our foreign policy, did it stop attacks? What I think they could be, and should be, involved in is—and by the way, one way to maybe solve that problem would be to have the DNI submit an affidavit, much like in other FISA contexts, that just asserts that there is foreign intelligence value and then he's held accountable for the accuracy of that.

But the things I do think the court ought to be able to look at in reauthorizing these procedures and the collection is, for example, how has the scope of the intercepts really worked? Are they collecting an unexpected volume of communications of Americans in the United States versus the things they're really targeting? How many errors have been made? What corrective procedures should there be in the process? I do think the court could meaningfully supervise that process.

Senator SPECTER. Thank you very much, Mr. Baker, Mr. Dempsey, Mr. Cunningham, and Ms. Spaulding, for taking the time to prepare statements and for waiting all morning to testify. Thank you.

Senator FEINGOLD. Thank you, Senator Specter.

Senator Whitehouse.

Senator WHITEHOUSE. I'd like to join Senator Specter in our thanks for the work that you've done. Ms. Spaulding, I thought your analysis was particularly thoughtful and helpful in tracking the actual plumbing, if you will, the legal, legislative language of the statute and where it overshot and where it missed.

It strikes me, I know there are witnesses from different backgrounds and orientations here, and we've just had Democrats and Republicans alike ask questions, we've had the DNI here. What I'm a little bit surprised by is how everybody seems to have come into an accord about where we need to be. There really does seem here to be a fairly sensible path that is relatively well illuminated by the exchange that took place between the members and the DNI, and what we've heard from all of you here today. Does that come as a surprise?

Mr. CUNNINGHAM. Well, Senator, just speaking for myself, all four of us have known each other in various capacities and worked together for a very long period of time, and I think have a lot of respect for each other. So I'm not terribly surprised. I would highlight one, I think, difference that I'm quite certain exists between folks on the panel, which the committee ought to think about for the future.

That is, under the Fourth Amendment, when you're talking about surveillance directed at targets overseas but which may—or

will, I guess—intercept certain communications of people in the United States, the difference between what I would call programmatic review and approval by the court, where the court supervises the kind of things I was talking about with Senator Specter, versus the requirement to get individual, particularized warrants in advance, I think that's probably worth exploring because I think we may have some differences on that.

Senator WHITEHOUSE. Although I suspect fewer than you imagine.

You said that there was a question about the scope of the Fourth Amendment when an American travels outside the boundaries of the United States. I agree that the decisions, at least that I have read, leave that an unanswered proposition.

Is that something that we should try to pin down or is it best to simply operate by analogy, create protections akin to those that are longstanding under Title 3, and then wait for the judicial process to eventually come through with decisions that further define the rights of an American traveling abroad? There are obviously less than at home, but it's not clear how less, at least from the point of view of the judicial decisions. I was surprised at how vague the law is on that question.

Mr. DEMPSEY. Well, Senator, I think that my reading of the current state of law is that at least an American citizen, and maybe a U.S. person abroad, has the protection of the Fourth Amendment in the sense that the reasonableness clause of the Fourth Amendment applies to an American abroad, but the warrant clause does not.

Senator WHITEHOUSE. But the warrant requirement doesn't.

Mr. DEMPSEY. Which was the holdings of the cases so far. Now, that doesn't mean, as Senator Specter and others were going, that Congress could not give a court jurisdiction to issue a warrant for surveillance abroad. In fact, at one point the Administrative Office of the U.S. Courts considered such a proposal for, I think, for a Rule 41—

Senator WHITEHOUSE. It was actually my suggestion.

Mr. DEMPSEY. That was your suggestion?

Senator WHITEHOUSE. That is one of my suggestions in this process.

Mr. DEMPSEY. I thought it had been previously floated and it hadn't gone forward. But I think that I heard sort of consensus on that. The DNI said he wanted to obviously see the language. I think that's the right direction to go.

Senator WHITEHOUSE. Once we've gotten to the point of the court being the right direction to go, when I did surveillance in the law enforcement context, what we needed to prove was that there was probable cause to believe that the individual target was engaged in a specified violation of the laws of the United States or the State, depending on who you were doing. In this case, the standard is different. The Attorney General is required to opine that there is probable cause to believe that the target is an agent of a foreign power. Is that the correct standard, and where does it come from?

Mr. DEMPSEY. Well, that's the standard in Executive Order 12333, and that's the one that the administration is living by, with

the Attorney General making that decision. So in essence, all we do—

Senator WHITEHOUSE. Does it have august history? Is that language that was crafted from other statutes and goes way back?

Mr. DEMPSEY. Well, I think "agent of a foreign power" has origin in the Keith case. I think for now, I think it's good enough.

Senator WHITEHOUSE. Ms. Spaulding, you were nodding your head.

Ms. SPAULDING. I was just saying it is. It's in a footnote in the Keith case. Really, where the Keith opinion is noting what it is not covering in the case, because it was a case of purely domestic, no indication of any international or foreign connection, they said. So our decision here is not addressing one way or another how this would apply if we were dealing with foreign powers or agents of foreign powers. That's where the language came from.

Senator WHITEHOUSE. May I ask one final question, Mr. Chairman? I know I'm over my time.

Senator FEINGOLD. Yes. Go ahead.

Senator WHITEHOUSE. One of the things that has struck me, as I've been involved in this or other contexts than you all have been, as technology has changed, the intrusion that the search warrant effects into somebody's privacy has expanded. Back when the founding fathers dreamed this up, the sheriff went into your house, he rummaged around, he grabbed the evidence that he needed. It was taken to the courthouse, it was used in the trial, and it was either disposed of or returned, end of story.

Then comes the Xerox machine. Now the sheriff or the police officer goes into the house, he grabs the relevant information and makes a copy of it, returns it when everything is done. And still in the file someplace down in the dusty basement of a courthouse is the stuff that was taken from your house, hard to find.

Now we get to the electronic age. Now they take it and they scan it and it goes into a data base, and the live intrusion into the house that was over and concluded back when the founding fathers wrote this, is actually preserved electronically forever, not only for those officers and the people in the case to look at, but for anybody who can have access to it to look at.

I'm interested in any thoughts that you may have. I'm opening a large discussion right now. But if you wouldn't mind, for the record, pointing me to things that you think discuss this issue intelligently and are things that we should consider as we continue to move into a more electronic age.

I think that the people who wrote the warrant requirement into the U.S. Constitution would be surprised to see the preservation of data that now exists and the research that continues to be done, hyphen searches that can be done once that materially has been grabbed once properly, but then stored. And I don't mean just in the intelligence context. This is just as true of an FBI, an ATF, Secret Service, or other search as it is in the intelligence context. A quick reaction, and then I'm holding everybody here.

Mr. BAKER. If I could, just briefly, Senator. I think you've put your finger on a very important point. But what I'd say is, although technology presents us with certain problems with respect to privacy, certain issues and concerns, technology also presents us with

certain solutions, certain tools that we might use to be able to do this. I mean, this is going to be—

Senator WHITEHOUSE. It's our job here to create those, to require the implementation of those tools, I guess.

Mr. BAKER. Tools. But I'm talking about technological tools that can be used to assist us in that way. What I would suggest or recommend is getting a briefing, perhaps, from the intelligence community on some of the minimization procedures that are in place now generally speaking and some of the changes that are afoot. You might find some of those interesting with respect to dealing with some of these issues.

If I could just go back to the prior question just very briefly, I would just signal a note of caution with respect to changes that you might want to make with respect to activities vis-a-vis Americans overseas, because there you need to be very careful with what you're doing and how you're impacting the activities of our intelligence officers and employees overseas. The overseas environment is very different from the domestic environment, when you're literally on the ground and doing things. There is legislative history on this. Congress has historically been concerned about this, but shied away from trying to legislate in this area because it is complicated. I'd be happy to provide—

Senator WHITEHOUSE. Yes. But what is not complicated about it is the statute that says that it's no longer electronic surveillance if it is a person reasonably believed to be outside the United States, and there's no FISA court restriction on a group of people that is that broadly defined.

As Admiral McConnell noted, that could include our troops serving in Iraq. I don't think moms and dads who send their sons over to serve in Iraq have any expectation that their son can have their e-mails, their telephone calls listened in to by the U.S. Government, willy nilly, without a warrant, without any protection. Ditto a family that takes a vacation down to Mexico, or somebody who goes across the Canadian border, or somebody who goes to Italy or Ireland to visit their family.

We have a strong expectation that when an American travels, there is a significant panoply of rights that comes with them, and that has not yet been well defined. Unfortunately, the definition in the Protect America Act is non-existent. I mean, it's just, as soon as you step over the borders, you're all done. We don't care. You've got no rights, you've got nothing.

So you have to look to other places to find those protections, like the executive order. But in this administration, who knows? It might be a secret executive order in somebody's man-sized safe that we don't even know about, you know.

Senator FEINGOLD. I'm going to move into another round myself, here.

Mr. Baker, as you've already indicated, many people are concerned with the potential breadth of the Protect America Act. I appreciate that Mr. Weinstein has sent a letter to Congress stating that the administration would not rely on some of these interpretations. But setting aside his letter for now, is it possible to read that law to permit a warrantless physical search or business records search in the United States?

Mr. BAKER. It's possible.

Senator FEINGOLD. And in your experience, do government lawyers ever read statutes aggressively?

Mr. BAKER. Well, it depends on who you speak to. There are lawyers in the community that take very aggressive stances on particular legal questions. It is late in the day, it's on a Friday evening, it's 5:00, something has to happen right away. That goes back to my earlier point about clarity and simplicity in the law. You put the folks who have to make a decision in difficult situations, if the law can be read in a certain way, it becomes very hard to say no to that kind of suggestion.

Senator FEINGOLD. As has been noted, the language in the PAA that has received a lot of criticism is where it authorizes the warrantless acquisition of information "concerning" people outside the United States. Do you see any justification for using the phrase "concerning"?

Mr. BAKER. Well, it gives you more flexibility. It's a term that gives more flexibility. But it implies more flexibility, maybe is a better way to say it. If they had used the word "targeting", which I think is probably a better word than either "concerning" or "directed at", quite frankly, but if you use the word "targeting", targeting is a word that has significance. It carries weight in the intelligence community. Folks generally know what that means.

Senator FEINGOLD. So you would not recommend using the term "concerning"?

Mr. BAKER. "Concerning" is a word that I think is perhaps of use. As I said earlier, is as a matter of concern.

Senator FEINGOLD. And should be eliminated in any more permanent version of this law.

Mr. BAKER. I think there are better and clearer words that could be chosen.

Senator FEINGOLD. OK.

Mr. Dempsey, your comment on that?

Mr. DEMPSEY. I agree entirely. I think we have passed beyond—hopefully passed beyond—the language of the Protect America Act and are now working to come up with something that is clearer.

Senator FEINGOLD. Ms. Spaulding, on that point?

Ms. SPAULDING. Absolutely. I agree, Senator.

Senator FEINGOLD. All right.

Ms. Spaulding, earlier today Director McConnell acknowledged that the Protect America Act would authorize the bulk collection of all communications originating overseas, including communications with Americans, if it were technologically possible to do that. Should we be concerned about that?

Ms. SPAULDING. Well, I thought it was interesting. The Director said two things. One, he seemed to say that it was not technologically feasible, but he also said that it would have to be within the definition of foreign intelligence or for foreign intelligence purposes.

And certainly I think as a matter of resource dedication, that is very likely the case. However, again, as a matter of statutory interpretation, 105(a) does not require that it have anything to do with foreign intelligence or be for foreign intelligence purposes. It simply defines all of those communications out of those statutory protec-

tions. So, it certainly would enable or not put any restrictions on the bulk collection.

I'm not sure that I have, necessarily, concerns with the bulk collection overseas of communications. I think where it really becomes important, obviously, is when you look at how you use that information. At what point do you dip into it? What kinds of searches can you conduct, when you start to conduct searches of all that information using U.S. person names, for example? What are the restrictions on your ability to retain that information, to disseminate that information? That's where I think all of the safeguards and protections that we've talked about today and elsewhere are very important.

Senator FEINGOLD. Thank you.

Mr. Baker, as a general matter, when this committee undertakes an overhaul of the statute, members are likely to examine judicial opinions or government briefs to understand how courts and government lawyers have interpreted the law thus far. Do you think that it would be helpful to this committee, in its consideration of changes to FISA, to understand fully how the Foreign Intelligence Surveillance Court and the executive branch have interpreted that statute?

Mr. BAKER. As a general matter, yes, consistent with the national security needs of the United States.

Senator FEINGOLD. Well, then do you think as a matter of course that Congress should have access to any significant legal decisions made by the FISA court in any form, as well as associated pleadings, which as you know often contain important legal arguments?

Mr. BAKER. I believe the significant legal opinion requirement is already in law. I believe that's already in FISA.

Senator FEINGOLD. Senator Whitehouse, do you have anything else?

Senator WHITEHOUSE. That's all.

Senator FEINGOLD. OK.

Well, I want to thank you all. You've been terribly patient. This has been an excellent hearing today. I thank you all. That concludes the hearing.

[Whereupon, at 12:49 p.m. the hearing was concluded.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

"Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?"
September 25, 2007

Questions for James A. Baker[1]

Questions for the Record Submitted by Ranking Member Arlen Specter

1. In Jack Goldsmith's recent book, The Terror Presidency: Law and Judgment Inside the Bush Administration, Mr. Goldsmith writes: "Jim Baker analogizes the task of stopping our enemy to a goalie in a soccer game who 'must stop every shot, for the enemy wins if it scores a single goal.' The problem, Baker says, 'is that the goalie cannot see the ball – it is invisible. So are the players – he doesn't know how many there are, or where they are, or what they look like. He doesn't know where the sidelines are – they are blurry and constantly shifting, as are the rules of the game itself.'" (Emphasis added) [sic].

a. Is Mr. Goldsmith right to credit you, among others, with the soccer goalie analogy?

Yes.

b. What does the goalie analogy portend for our decisions about whether to renew the Protect America Act? Specifically, what are we to do when NSA analysts and DNI McConnell tell us that they cannot know in advance whether a terrorist overseas will call into the US?

The goalie analogy as described above is meant in part to convey the idea that counterintelligence is a difficult and stressful business in many respects. The stakes are extremely high; the adversaries are smart, dangerous, and elusive; and the rules of the game are subject to change at any moment without prior warning. And even if the goalie is superb, sometimes the other team scores a goal. A good goalie, however, remains calm under pressure, directs his or her team with confidence, and uses all available assets to thwart the strategy and tactics of the opposing team.

In the world of counterintelligence, our intelligence professionals face many difficult challenges. They have many assets available to assist them in executing their responsibilities, however, such as sizeable financial, human,

[1] I appeared before the Committee at its request in my personal capacity. The views I express in response to the following questions for the record do not necessarily reflect those of my current or former employers. Pursuant to 28 C.F.R. § 17.18, the Department of Justice reviewed these responses for classified information.

53358.001

and technological resources. Other assets include our fundamental constitutional principles and the American values that underlie them, such as a commitment to justice, freedom, and the rule of law.

Obviously, we need surveillance laws that provide the Intelligence Community with the tools it needs to disrupt and defeat terrorist and other threats to our security. Those tools must be flexible and adaptable, but they must also provide the Intelligence Community with clear guidance about what the law is and who may be targeted for collection, and they must be consistent with American law and values.

With respect to your particular question about concerns that NSA and the DNI have expressed, my understanding is that they are now satisfied with the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended by the FISA Amendments Act of 2008. Nevertheless, there are several things about the legal regime applicable to foreign intelligence collection that concern me, especially the complexity of the laws that now apply to such intelligence activities. I discuss this issue in greater detail below in my response to one of the questions from Senator Kennedy.

2. Given your knowledge of the Foreign Intelligence Surveillance Court, how do you believe that the court would react to an expansion of its jurisdiction to include approval of surveillance targeting U.S. persons overseas – if, for example, the authority granted to the Attorney General under Section 2.5 of Executive Order 12333 was transferred to the court by statute?

My experience tells me that the court will adhere to the Constitution and laws of the United States. If it determines that the laws that Congress has enacted governing the collection foreign intelligence information that is targeted at United States persons abroad are consistent with the Constitution and are otherwise lawful, the court will not hesitate to enforce such laws.

Questions Submitted by Chairman Patrick Leahy

1. The Protect America Act changed the definition of electronic surveillance in FISA. What impact might this change have on FISA? Is the change necessary to accomplish the objectives of the PAA?

It is difficult to ascertain the precise need for the change to the definition of electronic surveillance reflected in section 105A of the Protect America Act. In any event, it is not clear to me that the change was necessary in order to implement the collection authorized under sections 105B and 105C of the Act. Indeed, the FISA Amendments Act of 2008 appears to have addressed the same underlying issue that the Protect America Act was intended to confront without amending the definition of electronic surveillance (although the construction provision found in 50 U.S.C. § 1881a(c)(4)

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00069 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.002

may represent an effort to effectively modify FISA's definition of electronic surveillance).[2]

One impact of the change was to make clear that government officials who directed surveillance at persons that they reasonably believed were abroad would not run afoul of the criminal prohibitions set forth in section 109 of FISA (50 U.S.C. § 1809), even if such surveillance involved purely domestic communications.

2. Please answer the following about the role of the FISA Court under the PAA:

> Can Congress provide for [a] more significant FISA Court role in oversight of the PAA without unduly burdening the Intelligence Community?
>
> ***Yes. In my experience, it is possible to have both expeditious collection of foreign intelligence information and robust oversight that includes a significant role for the FISA court. Congress mandated a more significant role for the FISA court in the FISA Amendments Act of 2008.***
>
> Does a "clearly erroneous" standard of review leave the Court a sufficient, substantive role?
>
> ***The "clearly erroneous" standard set forth in section 105C(c) of the Protect America Act obviously reflected the desire of Congress to restrict narrowly the scope of the court's review of the government's collection procedures. The FISA Amendments Act of 2008 adopts a different approach, which, in my view, is more likely to ensure proper and continuing court review of the government's collection activities to make sure that those activities adhere to the Constitution and laws of the United States.***
>
> Under the PAA, if the Court found the procedures that the Administration was using to determine "foreignness" were inadequate, what could it do?
>
> ***Under section 105C(c) of the Act, if the court found that the collection procedures were not reasonably designed to ensure that the acquisitions authorized under section 105B did not constitute electronic surveillance (because the surveillance was directed at a person reasonably believed to be located outside the United States), it could order the government to submit new procedures within 30 days or to cease any acquisitions under section 105B that were implicated by the court's order.***

[2] 50 U.S.C. § 1881a(c)(4) provides: "Nothing in title I [of FISA] shall be construed to require an application for a court order under such title for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States."

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00070 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.003

Questions Submitted by Senator Edward M. Kennedy

1. One thing the administration rarely mentions in its statements about the Protect America Act is the Fourth Amendment. Yet the Constitution is the supreme law of the land, and all legislation must comply with it. There is obviously some uncertainty in Supreme Court case law about the extent to which the Fourth Amendment limits electronic surveillance, but we know from cases like *Katz* and *Keith* that the Fourth Amendment does apply in many situations.

Questions:

- When Americans talk or e-mail with people overseas, does the Fourth Amendment provide any protection for their international communications?

An assessment of the nature and scope of the Fourth Amendment protections applicable in any particular situation necessarily involves consideration of many factors, including a person's reasonable expectation of privacy in the communications at issue, the type and extent of the governmental intrusion, and the purpose for the intrusion. My current understanding of the best reading of the law is that: (1) the government's collection of the international and foreign communications of United States persons (that is, American citizens, permanent resident aliens, and certain corporations and associations) for foreign intelligence purposes must comport with the reasonableness clause of the Fourth Amendment; and (2) the warrant clause of the Fourth Amendment does not apply to the collection of such communications for foreign intelligence purposes.

- In your view, does the Protect America Act comply with the Fourth Amendment? If not, what are its offending provisions?

In my view, it is likely that a court would find that the Protect America Act comports with the reasonableness clause of the Fourth Amendment and is therefore constitutional with respect to the acquisition of international and foreign communications. Whether a court would find that the Act is reasonable under the Fourth Amendment with respect to the collection of purely domestic communications would depend on many factors, including whether the court believed that a warrant was required to conduct such collection, factual considerations such as the design and implementation of the acquisition procedures that the Act requires, and the purpose of the collection.

- What role should the FISA court have in safeguarding Americans' Fourth Amendment rights?

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00071 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.004

In my view, the FISA court has played a critical role in protecting the safety and liberty of the American people both before and after 9/11. Although some have criticized it as slow, inefficient, and cumbersome, in my experience the exact opposite is true. In my dealings with the court from 1996-2007, I found it to be highly sensitive to the needs of the executive branch to obtain important foreign intelligence information on a timely basis; adept at interpreting the law and established rules and procedures to address changes in technology and in the threat environment; and steadfast in protecting the legitimate privacy interests of Americans. Thanks in large measure to the flexibility, creativity, and common sense of the FISA court – as well as the dedicated professionals of the Office of Intelligence Policy and Review (OIPR) – the FISA process worked during wartime. As a result, the Nation was protected from foreign threats, as well as from government overreaching. The FISA process produced a large volume of critical actionable intelligence, and works best when there is robust coordination and information sharing among intelligence agencies.

In appropriate circumstances, the court should conduct a meaningful review of the government's proposed collection activities before they occur; approve, modify, or disapprove those proposed activities; and then closely monitor the government's compliance with the applicable approval and related procedures and guidelines. When utilized properly, the FISA court can make significant contributions to protecting both the security and liberty of the American people.

2. As you know, the Protect America Act weakens the role of the Foreign Intelligence Surveillance Court. For communications covered by the Act, the FISA court is permitted to conduct only a very general review of the government's collection procedures, long after the fact, under a "clearly erroneous" standard. That's a far cry from the central role that the Court has been playing under FISA.

The Administration has attempted to justify its undermining of the FISA court by claiming that more serious judicial review would be too burdensome, and that executive branch oversight is sufficient to make sure the law is not abused.

Questions:

- How do you regard the Administration's arguments for why the FISA court should be marginalized?

Please see my answer to question 1 above.

- What role should judicial review have under any new legislation?

Please see my answer to question 1 above.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00072 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.005

3. Congressional oversight under the Protect America Act is also weak. Reports are made to Congress semi-annually. The only information that the Administration has to provide is the number of certifications and directives issued during the reporting period and descriptions of incidents of non-compliance.

Questions:

- Are these reporting requirements adequate to ensure that Congress understands how the statute is affecting Americans and has the information necessary to fulfill its oversight responsibilities?

The reporting requirements set forth in section 4 of the Protect America Act are very limited. The reporting requirements set forth in the FISA Amendments Act of 2008 are considerably more robust than those in the Protect America Act.

- What information does Congress need to conduct real oversight?

As I discussed in a piece that I wrote for the Harvard Journal on Legislation,[3] effective oversight of the Intelligence Community is difficult for many reasons. If Congress is serious about conducting effective oversight, among other things: (1) members – especially those on the intelligence committees – must devote the time and energy necessary to learn the facts and the issues sufficiently so that they can ask probing follow-up questions in response to Intelligence Community testimony and briefings; (2) the intelligence committees must hire and retain sufficient numbers of experienced staff who can delve into critical issues in significant detail and who have the time to go out into the field to assess how intelligence activities are conducted; (3) Congress should enact legislation that mandates investigations and reports by pertinent inspectors general; and (4) Congress must earn and maintain the trust of the Intelligence Community by scrupulously avoiding public comment on sensitive intelligence matters unless such disclosures are critical to informing the public about abuses or misleading public statements by executive branch officials.

Specifically with respect to surveillance, Congress needs to pay close attention to the matters raised in the various reports that the Attorney General sends to Congress on a regular basis. Members and their staff must read the reports closely, and request informative follow-up briefings from the government to make sure that Congress understands the full context and importance of the matters raised in the reports.

In addition, congressional staff should meet frequently with a variety of relevant supervisors and line officials, and request and review redacted versions of surveillance applications and other documents to gain a better understanding

---

[3] *See* James A. Baker, *Symposium Introduction – Intelligence Oversight*, 45 Harvard Journal on Legislation 199 (Winter 2008), *available at*: http://www.law.harvard.edu/students/orgs/jol/vol45_1/baker.pdf.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00073 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.006

of how the process works and what level of factual predication the government and the FISA court deem adequate to meet various applicable legal standards such as probable cause.

4. The Administration is demanding that Congress grant retroactive immunity for communications service providers that complied with unlawful surveillance requests. Some of these companies apparently cooperated with the warrantless surveillance program, which violated FISA.

Questions:

- How do you regard the Administration's argument that these companies must be granted full immunity or else they will go bankrupt? Aren't there other ways – such as a cap on damages – to prevent bankruptcy while still holding companies liable for violations of FISA?

Congress enacted immunity provisions for certain service providers in the FISA Amendments Act of 2008 so no response is necessary to this question.[4]

- If bankruptcy is not the real issue, why is the Administration so adamant that retroactive immunity must be provided?

Please see the answer to the question immediately above.

- Do you agree that provider liability is a key structural protection of FISA?

Please see the answers to the questions immediately above.

5. Many of us are obviously concerned about the scope of the Protect America Act. The Act isn't clear in many respects, but it seems to authorize very broad warrantless surveillance – far broader than anything allowed under FISA.

Questions:

- Under the Protect America Act, would it be lawful to collect every communication from America to Germany – without a court warrant – if the purpose of this collection was to find one terrorist in Germany?

In my view, it is possible to read the Protect America Act to permit such collection.

[4] Please note that my current position is Assistant General Counsel for National Security at Verizon Business. As discussed above, the views expressed herein are strictly my own and do not necessarily reflect those of my employer.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00074 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.007

○ How could the Act be amended to place some constraints on such activity?

The Protect America Act itself placed some constraints on such activity by requiring, for example, that the government use minimization procedures with respect to acquisition activity approved under the Act. The implementation and proper use of appropriate minimization procedures are critically important to protecting the privacy of United States persons when the government must (or is permitted to) obtain authorizations to collect information and communications on a large scale.

In my experience, effective minimization procedures are essential to protecting the constitutional rights of Americans while at the same time ensuring that the government obtains the foreign intelligence information it needs to protect the country. FISA's current definition of minimization procedures (found at 50 U.S.C. § 1801(h)) reflects an effort to balance the degree of governmental intrusion – by limiting the acquisition, retention, and dissemination of information concerning United States persons – with government's need to obtain, produce, and disseminate foreign intelligence information.

In general, Congress should make sure that: (1) the government develops and implements appropriate minimization procedures; (2) the procedures require destruction of non-pertinent material after a reasonable – but defined – period of time (such as five years after collection); (3) the FISA court reviews the procedures in advance and makes sure that government is following those procedures in practice; (4) inspectors general regularly review the collection activities that the government conducts under the minimization procedures; and (5) Congress conducts active oversight of the government's minimization practices.

• Does the Protect America Act cover stored communications – for instance, e-mails sitting in a person's mailbox – as well as real-time communications?

Yes, it covers both stored communications and communications collected "in transit."

○ Is this a significant change in the law? Why does it matter?

FISA previously permitted the collection of stored communications, either as "electronic surveillance" or a "physical search" as those terms are defined in the Act.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00075 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.008

An important change in the Protect America Act is that it allowed the government to acquire stored communications and communications in transit without an individualized probable cause finding in advance by a judicial officer. The authority for approving such acquisitions was shifted from the court to the Attorney General and the Director of National Intelligence.

• Why did the Administration insist on the phrase "concerning," rather than "directed at," when describing surveillance in Section 105B? Isn't "concerning" a significantly broader term?

I was on leave from the Department of Justice at the time that the Protect America Act was enacted so I do not know exactly what the government asked Congress to enact.

It is unclear to me exactly why section 105A uses the term "directed at," while section 105B uses the term "concerning." The term "concerning" seems to be much broader in scope than the term "directed at," which is more similar to "targeted at." The term "concerning" would include communications to, from, or about a person, or information from whatever source that pertains to a person. As a result, under the Protect America Act the government could acquire an e-mail that was to or from a person who was of foreign intelligence interest, as well as communications to or from third parties who mention or discuss the person of interest.

• In general, would you say that the Protect America Act simply "modernizes" FISA to account for changes in technology and security threats? Or does the Act overturn FISA in key respects?

The Protect America Act "modernized" FISA in the sense that it eliminated the need for the government to obtain individualized probable cause determinations from a judicial officer in advance in certain circumstances.

6. The Administration has repeatedly claimed that the Protect America Act restores FISA's original intent. One aspect of this claim is that FISA was never intended to protect Americans who communicate with foreign targets. Director of National Intelligence McConnell has stated that "Congress crafted [FISA] specifically to exclude the Intelligence Community's surveillance operations against targets outside the United States, including where those targets were in communications with Americans, so long as the U.S. side of that communication was not the real target."

Questions:

• Is this claim by the Administration correct?

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00076 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.009

It is difficult to discern exactly what Congress understood about the state of technology in 1978 and what it intended to cover (or exclude from coverage) in the original FISA.[5] Without recounting the complex history of the original Act, suffice it to say that Congress clearly intended that: (1) FISA would not apply to certain international and foreign communications – such as international telephone communications transmitted via satellite (even if one party is in the United States) as well as wire communications that are to and from abroad but that transit the United States; and (2) FISA would apply to at least some international communications of Americans, even if the government was targeting persons located abroad.

In particular, one of the original FISA's four definitions of electronic surveillance is "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States." 50 U.S.C. § 1801(f)(2). Under that definition, even if the government was targeting a person overseas, FISA would regulate the collection if the government collected communications to or from a person inside the United States, so long as the acquisition occurred here.

• Even if the Administration's claim is correct, do you think it's appropriate to provide as little protection as this statute provides for Americans whose communications may be "incidentally" collected by the government?

The government's acquisition – that is, seizure – of the communications of United States persons is always governed by the reasonableness clause of the Fourth Amendment. So long as the government employs adequate minimization procedures when it inevitably seizes such communications incidental to its collection activities that are targeted at non-United States persons who are abroad, the government's conduct should comport with the Fourth Amendment. This is why it is critical for Congress to conduct rigorous oversight of the government's minimization practices.

7. Under the Protect America Act, it is possible that millions of "incidental" communications between foreign targets and innocent American citizens will be collected by the government. Many of us are concerned that the Intelligence Community's minimization procedures – the procedures that control what can be done with information after it has been collected – are insufficient to protect the privacy of these Americans.

---

[5] For one account of this history from outside the government, *See* David S. Kris, "Modernizing the Foreign Intelligence Surveillance Act," Brookings Institution (2007), *available at*: http://www.brookings.edu/~/media/Files/rc/papers/2007/ 1115_nationalsecurity_kris/ 1115_nationalsecurity_kris.pdf.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00077 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.010

Questions:

• To the best of your knowledge, what limits currently exist on the government's ability to store, analyze, and disseminate information it collects without a FISA warrant on Americans who were never a target?

FISA defines the term "minimization procedures" in part as follows:

> ***[S]pecific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose[s] and technique of the particular surveillance [or physical search], 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 . . .***

See 50 U.S.C. §§ 1801(h)(1) and 1821(4). As a result, the key limitation in the Act is that the minimization procedures must be "reasonably designed" to protect the privacy of United States persons and, at the same time, permit the government to collect and disseminate foreign intelligence information. Whether the minimization procedures that the government utilizes are in fact reasonable is determined by both the Attorney General and the FISA court. The minimization procedures may vary depending upon the type of collection at issue, as well as the likelihood that the government will collect United States person communications or information in any particular circumstance. For example, the minimization procedures applicable to microphone surveillance of a residence in the United States should probably differ from those applicable to surveillance targeted at the telephone communications of non-United States persons located abroad. If Congress is interested in closely monitoring the government's minimization practice, it must obtain unredacted copies of the procedures themselves, and ask the government for reports on how it implements those procedures in various factual settings.

• Should new legislation require stronger minimization procedures, either for all Americans' communications or at least for international communications that are "incidentally" collected?

As noted above, under FISA the government must minimize all United States person communications, including international communications that the government acquires. Congress must review the actual procedures themselves – as well as the manner in which the government implements them – to determine whether it is satisfied with how well the current structure protects the privacy of Americans. To my mind, this is really a fact-specific oversight question rather than a legislative matter. Congress should focus on the rules regarding: the nature and scope of the data the government can collect; who has access to the collected data and under what circumstances can they access it; the permitted

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00078 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.011

dissemination of such information to federal, state, local, and foreign authorities; and when non-pertinent information that the government has collected is destroyed.

8. It appears from the text of the Protect America Act that Americans who travel abroad are now extremely vulnerable to warrantless surveillance. When Americans travel out of the country, the Act suggests that the government can wiretap them – without any warrant – as long as a significant purpose of the surveillance is to obtain foreign intelligence information.

Questions:

- Is this correct?

Yes.

- Can you explain what effect Executive Order 12333 has on the wiretapping of Americans abroad, and whether this Order will continue to have force under the Protect America Act?

My understanding from publicly available information is that the government continued to apply section 2.5 of Executive Order No. 12,333 during the effective period of the Protect America Act. Since the enactment of the FISA Amendments Act of 2008, such collection activities are now governed by 50 U.S.C. §§ 1881b and 1881c.

- To protect the rights of Americans who travel abroad, should we require a warrant anytime the government wants to target a U.S. citizen?

As noted above, such collection is now governed by 50 U.S.C. §§ 1881b and 1881c.

9. We spent much of the hearing debating the Protect America Act, which is very controversial and troubling in itself. But the Administration is also acting for additional changes in the FISA law. For example, Director McConnell has asked for a variety of "streamlining" measures and for an extension of FISA's emergency provision from 72 hours to one week.

Questions:

- What do you think of these new requests?

In my view, most of the changes that the government proposed – some of which Congress enacted in the FISA Amendments Act of 2008 – will not significantly streamline the FISA process. The most significant change that Congress made

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00079 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.012

in terms of expediting the processing of FISA applications was to permit the Deputy Director of the FBI to sign the certifications that are filed as part of an application (although it must be noted that this change lowers the level of accountability for the nature and purpose of the collection to an official who is not Senate-confirmed).

• Beyond this debate we are having over FISA and the Protect America Act, what else does Congress need to do to ensure that our intelligence programs are as effective and responsible as possible?

In order to better ensure that our intelligence programs are as effective and responsible as possible, Congress should consider the following:

1. What threats do we face? Before Congress can address any other questions, it must first ensure that it has an adequate understanding of the foreign and domestic threats that the United States faces today, and is likely to face in the foreseeable future. Obviously, Congress must rely to a significant degree on the Intelligence Community for an assessment of those threats. Indeed, Congress receives comprehensive periodic threat assessment testimony and briefings from the Intelligence Community. While Congress must afford great deference to the judgments of intelligence professionals, Congress should also obtain the views of outside experts from academia, think tanks, the private sector (which has a vested financial interest in accurately assessing the international risk environment), and the media, all of whom have important perspectives on domestic and foreign developments and can test the Intelligence Community's assumptions and conclusions. As the Director of National Intelligence has stated, "[t]he nation . . . requires more from our Intelligence Community than ever before, and consequently we need to do our business better, both internally, through greater collaboration across disciplines and externally, by engaging more of the expertise available outside the Intelligence Community."[6]

Accordingly, the next Congress should hold a series of open and closed hearings in early 2009 where it can hear from the Intelligence Community as well as outside experts on the nature of the threat environment. Such hearings will assist the Congress and the next Administration in establishing appropriate priorities for intelligence activities in the next few years.

Correctly assessing the threat environment, and then establishing national priorities based on such assessments, is akin to the Intelligence Community's process for establishing requirements for collection. The world is vast, so the Intelligence Community and Congress must make some educated guesses about what is important to the country and its interests so that the government can more effectively use all available resources.

---

[6] *See, e.g*, J. Michael McConnell, Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee* (February 27, 2008) at 2, *available at* http://www.odni.gov/testimonies/20080227_testimony.pdf.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00080 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.013

2. Do we have enough of the right people in the right jobs to deal with the threat environment? Our people are our most valuable resource. We can deal most effectively with the threat environment only if we have the right people in the right jobs working hard to get it right. And we must ensure that national security officials foster organizational cultures that reward creativity, diligence, analytical rigor, impartiality, and cooperation, and encourage appropriate risk taking consistent with the letter and spirit of the law.

For example, Congress must make sure that the people that the next Administration nominates to key national security positions are experienced and objective professionals with unquestionable integrity. And, as others have pointed out, the Senate must act quickly on nominations that the next Administration sends to the Hill. In addition, Congress should monitor closely appointments to key positions that are not subject to Senate confirmation.

Further, Congress must make sure that the Intelligence Community has funding for, and hires and trains, adequate numbers of competent intelligence professionals to do the work of the community. As I testified before the Committee in April 2008:

> *We must ensure that we have enough of the right people in our intelligence agencies to translate, analyze, and act upon all of the intelligence information that we collect. A successful intelligence system has four essential elements: requirements, collection, analysis, and production. We have to seek and collect the right information at the right time – that is, we want timely and accurate intelligence about the right topics – but we also need to process, store, translate, review analyze, produce, and disseminate that intelligence so that military commanders, CIA case officers, and FBI special agents can take prompt action based on it. Poor intelligence is distracting junk, and old intelligence is history.*
>
> *Advanced information technology systems assist in acquiring, processing, and assessing collected information, but they cannot do the analysis on their own. Only adequate numbers of highly trained and dedicated linguists, analysts, and agents who know their targets well can draw reasonable inferences from the facts, make prudent judgments based on the quality of the intelligence available, and make sound predictions and recommendations to policy-makers.*
>
> *Moreover, the task is especially hard because, as some have noted, the needle you are looking for is broken into many pieces and most of the pieces are disguised to look like hay. Spies and terrorists don't always identify themselves clearly when they are communicating, they use code words and obscure references to convey meaning, and they rely on a*

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00081 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.014

variety of communication modes to transmit messages. More collection will mean more dots available to connect. But intelligence officials will need to do the hard work of connecting them.

3. Do we have the right laws in place to deal with the threats we face and to preserve our constitutional rights? Since 9/11, Congress has amended the law in many respects to address important national security challenges that we now face. Much work, however, remains to be done.

In particular, Congress should simplify the legal regime for collecting foreign intelligence information. The legal framework that governs the collection of such information (both content and non-content, also known as "metadata") includes not only the Foreign Intelligence Surveillance Act of 1978, as amended, but also Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and the Electronic Communications Privacy Act of 1986 (which includes the Stored Communications Act). Unfortunately, the recent FISA Amendments Act of 2008 did not simplify this legal structure; indeed, it made it significantly more complex.

To put it plainly, these intertwined laws establish a complex, confusing, and redundant legal regime that regulates the government's intelligence collection activities. In some cases, it is exceedingly difficult to understand and implement these laws coherently, consistently, and quickly. This complexity puts the security of our nation at risk because intelligence professionals may decline to act when faced with legal uncertainty and potential criminal and civil liability, and it also increases the likelihood that intelligence agencies will inadvertently violate the law as they engage in collection activities or look for shortcuts around what may be viewed as incomprehensible and pointless legal impediments.

Moreover, the laws that are in place are not sufficient to deal with the rapid changes that are occurring (and will continue to occur) with respect to the ability of the government entities to collect, retain, and disseminate vast quantities of personal information about the lawful activities of Americans. As I have stated previously, "at some point in the future any human endeavor that can be represented by digital information will be recorded and stored by someone – either for commercial or public safety reasons – and sooner or later the government will want to acquire some or all of it for foreign intelligence purposes."[7] Our laws do not protect adequately the legitimate privacy interests of Americans in this regard and must be brought up to date.

In order to address this situation in as non-partisan a manner as possible, Congress could establish either a national commission or a joint congressional committee to review all federal statutes that regulate intelligence collection and

---

[7] *See* James A. Baker, *Symposium Introduction – Intelligence Oversight*, 45 Harvard Journal on Legislation 199, 208 (Winter 2008).

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00082 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.015

make recommendations on reforming the law, or it could ask the Administration for such proposals by a specified date. In any event, Congress should act promptly so that it can enact appropriate laws well in advance of the expiration of important parts of the FISA Amendments Act on December 31, 2012.

4. Are our intelligence, diplomatic, law enforcement, military, and economic activities coordinated sufficiently to deal with the threat environment? Although coordination and information sharing among elements of the Intelligence Community and other national security entities has improved significantly since 9/11, much work remains to be done. It is possible that Congress can legislate further in this area to mandate effective coordination and dissemination of intelligence information – such as by more clearly setting forth the budgetary and personnel authorities of the Director of National Intelligence. Most of the changes that are necessary, however, will come only through sustained congressional oversight that closely monitors the government's efforts in this regard. This is critical because, in my view, ineffective coordination, conflicting intelligence and law enforcement priorities and activities, and turf battles waste precious time and resources and risk compromising sensitive sources and methods. Poor coordination of intelligence activities may be our Achilles heel in our counterintelligence and counterterrorism efforts; effective coordination could be our ace in the hole.

5. Is the Executive Branch conducting proper oversight of intelligence activities? Congress must make sure that Executive Branch agencies have adequate financial and personnel resources to conduct robust oversight of our intelligence agencies. It must also make sure that there are competent, professional, and non-partisan personnel in key oversight positions, such as the general counsels and inspectors general at the various intelligence agencies. As former Supreme Court Justice and Attorney General Robert H. Jackson stated, "Fundamental things in our American way of life depend on the intellectual integrity, courage and straight thinking of our government lawyers. Rights, privileges and immunities of our citizens have only that life which is given them by those who sit in positions of authority."[8]

Congress should also make sure that the Executive Branch conducts regular reviews of all ongoing intelligence operations to ensure that such activities constitute appropriate uses of the limited resources that are available in light of the current threat environment, and that such activities are consistent with law and applicable policies, guidelines, and directives. Such a review will be especially important for the next Administration to ensure that our intelligence activities are consistent with the next President's policies.

---

[8] *See* Robert H. Jackson, *Government Counsel and Their Opportunity*, 26 A.B.A.J. 411, 412 (1940), *quoted in* Note, *Government Counsel and Their Obligations*, 121 Harv. L. Rev. 1409, n. 5. (2008).

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00083 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.016

6. Are we making full use of all available technological resources to collect, analyze, and share intelligence information? Are we effectively protecting our critical infrastructure? Are we planning for technological changes that will likely occur in 5-10 years? Our extensive reliance on technology, as well as our technological prowess, provide us with significant advantages over our adversaries, but also expose us to significant risks.

Although the Intelligence Community has made great strides since 9/11 in making more effective use of technology to identify threats, collect and analyze pertinent information, and share operational and finished intelligence among our national security entities and with our foreign partners, much work remains in this regard. It is probably prudent to have competition and diversity among intelligence agencies with respect to the utilization of information technology to minimize the risk of wide-spread, simultaneous failures brought about by technical flaws or hostile acts, but it is also important to have a coordinated approach to technology so that agencies can learn from the experiences of others. Congress must conduct effective oversight of the use of technology, and ensure that the Intelligence Community has adequate resources – either in-house or through contractors – to fully utilize available information technology but also to see that it does not waste those precious resources (both human and financial) on ill-conceived projects.

With respect to the protection of critical infrastructure, as discussed above Congress must ensure that it has as complete a view as possible of the threats that we face from potential conventional and cyber attacks to our critical infrastructure facilities. Assuming that the threat is real and pervasive, we must ensure that we are taking the proper steps to mitigate the risks. Public statements about the President's January 2008 comprehensive cyber security initiative that is reflected in NSPD-54 and HSPD-23 indicate that it is a step in the right direction.[9] Congress must closely monitor the progress of that initiative and ensure that it addresses technological changes that are anticipated in the immediate future. If necessary, Congress should also consider additional legislation to require further cyber security efforts.

7. Do we have the best organizational structure to deal effectively with our adversaries? Although Congress must remain diligent to make sure that our intelligence agencies are organized as optimally as possible, further reorganization efforts at this juncture would be counterproductive. In other words, the next Congress and Administration should not focus immediately on another reorganization of our national security apparatus. We need to let the dust settle from prior reorganizations before we undertake new ones. And the other priorities that I have set out above are much more important to address immediately than is further reorganization.

---

[9] *See, e.g.,* J. Michael McConnell, Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee* (February 27, 2008) at 16, *available at* http://www.odni.gov/testimonies/20080227_testimony.pdf.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00084 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.017

That said, it is prudent for Congress to continually assess the costs and benefits of prior reorganizations to ensure that relevant government agencies are funded, organized, and staffed appropriately to deal with today's intelligence and oversight challenges.

8. Are we prepared to deal with the results of intelligence failures? Are we planning for the worst? Congress and the American people must recognize that effective intelligence activities are only one part of our national response to the threats that we face, and that intelligence alone cannot keep us safe. Indeed, intelligence is such a difficult business that although we may say that failure is not an option, it is unfortunately a possibility. As a result, we must make sure that we have in place the policies, procedures, contingency plans, resources, and laws to deal with national crises, including catastrophic terrorist attacks.[10]

○ It has been reported that the National Security Agency is having many problems with management and with computational and translational aspects of intelligence analysis. Should these be priorities?

Yes – please see my answer to the question immediately above.

• Unfortunately, a majority of this Committee is hampered in this debate by not knowing precisely what we are fixing. Despite subpoenas, we have bee denied the legal justifications for the warrantless surveillance program, and we have been denied access to the FISA court opinions that we are told made new legislation necessary. We are being told we need to fix a problem whose nature and scope have not been revealed to us.

○ Given the secrecy that enshrouds this entire debate, how would you recommend Congress fulfill its oversight responsibility?

As I discussed in the above-referenced oversight piece that I wrote for the Harvard Journal on Legislation, there are certain structural impediments that make it difficult for any Congress to conduct oversight of intelligence activities. It is particularly important that that all members of Congress have confidence in the activities of the intelligence committees of both houses. The members and staff who serve on such committees must conduct themselves in a professional, non-partisan, and discrete manner at all times.

---

[10] *See* Ted Gistaro, National Intelligence Officer for Transnational Threats, *Remarks at the Washington Institute for Near East Policy, Washington, D.C.*, (August 12, 2008), *available at* http://www.odni.gov/speeches/20080812_speech.pdf ("[Al Qaeda a]ttack planning continues and we assess it remains focused on hitting prominent political, economic, and infrastructure targets designed to produce mass casualties, visually dramatic destruction, and significant economic and political aftershocks.").

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00085 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.018

○ Do you think Congress should conduct a broader review of intelligence policy at this time?

Yes. Please see my lengthy answer above to the question regarding effective and responsible intelligence programs.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00086 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.019

MORGAN & CUNNINGHAM LLC
ATTORNEYS AT LAW

CLAROLD F MORGAN
C FORREST MORGAN, III
H BRYAN CUNNINGHAM

5299 DTC BOULEVARD, SUITE 1350
GREENWOOD VILLAGE, COLORADO 80111

TELEPHONE (303) 743-0003
FACSIMILE (303) 743-0005

August 26, 2008

The Hon. Arlen Specter
Ranking Minority Member
Judiciary Committee
United States Senate
Washington, D.C. 20510

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

Re: Questions for the Record

Dear Chairman Leahy and Ranking Member Specter:

On August 19, 2008, I received a letter from Chairman Leahy notifying me that I was to be given seven (7) days to respond to ten (10) substantive questions concerning highly complex questions of constitutional and foreign intelligence surveillance law. Thank you for your opportunity to respond to these questions. My response follows immediately below.

Question for the Record Submitted by Ranking Member Arlen Specter

"At the hearing, I asked you about the possibility of requiring the government to report back to the Foreign Intelligence Surveillance Court periodically about the surveillance conducted pursuant to the Protect America Act. You expressed concerns about having the court 'evaluate the foreign intelligence value of the information' collected. Nevertheless, you suggested that it may be appropriate to have the court evaluate whether 'the scope of the intercepts really worked' as contemplated. Could you elaborate on the type of review you would consider appropriate when the court is asked to reauthorize the government's surveillance procedures, including the appropriate standard of review?"

As the Judiciary Committee is aware, a long line of United States Supreme Court and other United States federal court decisions speak to the critical separation of powers issues raised when the courts or Congress attempt to intrude on a "core" constitutional responsibility of the Executive Branch such as the conduct of foreign intelligence operations.[1] The overwhelming weight of constitutional and legal authority on this issue strongly supports the near-plenary

[1] For discussion and case citations of a number of important national security separation-of-powers decisions, see my letter to then-Chairman Specter and Ranking Member Leahy of February 3, 2006, reprinted for the Committee's convenience at the end of this letter, and available at www.morgancunningham.net.

53358.020

authority of the Executive Branch to manage, evaluate, and protect the results of, foreign intelligence operations and information. Based on these concerns, and numerous United States court decisions concerning the role of the Judiciary more generally, as well as timeliness and operational considerations, I am, as I testified, skeptical about the constitutionality and feasibility of the Foreign Intelligence Surveillance Court (FISC) to second guess the Executive Branch on the foreign intelligence value of information collected pursuant to foreign intelligence collection operations.

That said, in my judgment, and based on my strong belief in the value of checks and balances, it might well be appropriate and beneficial for the FISC to make determinations about, for example: whether ongoing foreign intelligence collection operations conducted to FISC orders are providing information concerning the targets and subject matters sought in application documents; whether collections operations are striking the appropriate balance between intrusiveness, breadth and type of communications intercepted; the ongoing efficacy of continued interceptions under original application conditions; and whether modifications in the collection activities might be warranted.

The proper constitutional balance in this area is delicate and the limited number of FISC judges available at any given time likely will preclude – at least under current threat conditions – deep, meaningful review of many of these issues in a timely way. Therefore, in my view, the standard of review should be highly deferential to the Executive Branch and mindful of the operational and timeliness requirements vital to defeating grave threats to our national security.

Remaining Questions

The remaining questions posed to all panelists, as articulated in Chairman Leahy's August 14, 2008 letter, relate exclusively to specific provisions of, or issues regarding, the Protect America Act (PAA), and/or to various reform proposals before the Senate nearly one year ago. After the Senate overwhelmingly approved legislation superseding the PAA, and this legislation became federal law last July, the remaining questions posed to me are largely or completely moot. This new law (the FISA Amendments Act of 2008), as you know, includes significant changes from the PAA, including new court involvement and protection for civil liberties. The Foreign Intelligence Surveillance Act, as amended by this new law, in my judgment strikes the balance recommended in the February 5, 2006 Op-Ed I authored with Dan Prieto.[2]

While it would be counterproductive at this point for me to respond specifically to the many detailed questions about the now-superseded PAA, many of the underlying Fourth Amendment,

[2] The Eavesdropping Debate We Should Be Having, available at: http://belfercenter.ksg.harvard.edu/publication/1512/eavesdropping_debate_we_should_be_having.html?breadcrumb=%2Fexperts%2F920%2Ferica_chenoweth%3Fback_url%3D%252Fpublication%252F18115%252Fhomeland_security%253Fbreadcrumb%253D%25252Ftopic%25252F100%25252Fgovernance%25253Fpage%25253D6%26back_text%3DBack%2520to%2520publication

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00088 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.021

separation of powers, and other crucial constitutional and practical questions are addressed in my February 3, 2006 letter to the U.S. Senate (reprinted below), and in the following materials:

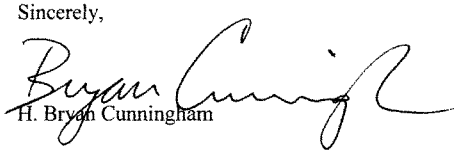
http://www.morgancunningham.net/article_38.pdf

http://www.morgancunningham.net/article_29.pdf

http://belfercenter.ksg.harvard.edu/publication/1512/eavesdropping_debate_we_should_be_having.html?breadcrumb=%2Fexperts%2F920%2Ferica_chenoweth%3Fback_url%3D%252Fpublication%252F18115%252Fhomeland_security%253Fbreadcrumb%253D%25252Ftopic%25252F100%25252Fgovernance%25253Fpage%25253D6%26back_text%3DBack%2520to%2520publication

Thank you again for the opportunity to testify before the Senate Judiciary Committee and to respond to the questions posed in Chairman Leahy's August 14, 2008 letter. I hope my responses, and the attached and referenced materials, will be of assistance should the important issues addressed arise again in the future. As indicated above, for your convenience, I attach below my signature the text of the letter I provided to the Committee in February 2006 addressing the important constitutional issues surrounding legislative attempts to regulate the collection of foreign intelligence information.

Sincerely,



H. Bryan Cunningham

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00089 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.022

February 3, 2006

The Hon. Arlen Specter
Chairman
Judiciary Committee
United States Senate
Washington, D.C. 20510

The Hon. Patrick Leahy
Ranking Minority Member
Judiciary Committee
United States Senate
Washington, D.C. 20510

Re: *Additional Constitutional Authorities Relevant to NSA Electronic Surveillance of International Terrorist Communications*

Dear Chairman Specter and Senator Leahy:

I am a former career national security lawyer and Central Intelligence Agency officer, now in private practice, after serving more than six years in the CIA and Department of Justice under President Clinton and, from May 2002 – August 2004, as Deputy Legal Adviser to President George W. Bush's National Security Council ("NSC").[1] I write to provide additional perspective, and to identify several important constitutional principles not yet widely discussed in published legal analyses, with regard to the recently disclosed National Security Agency ("NSA") program to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations (the "NSA Program").[2] Because of the importance of these constitutional principles, I urge Congress to consider the analysis, and legal authorities identified, in the remainder of this letter as you debate this critical issue.

Executive Summary

Even assuming, though we do not yet know all the facts, that at least some aspects of the NSA Program were not consistent with the procedural strictures laid down by Congress in FISA, published legal analyses to date by the Commentators (as defined in endnote 8) are fatally flawed, as follows:

- Two centuries of Supreme Court and other legal precedent strongly suggests that the National Security Agency program to intercept international communications of foreign terrorists is consistent with the Constitution and, therefore, lawful;

- The Commentators generally argue that that the President is *completely foreclosed* from exercising the "core" of his "plenary" constitutional foreign affairs authority -- that is, the collection of foreign intelligence -- except when complying with each and every provision of FISA, even if, as applied to the narrow facts and circumstances of the NSA Program, FISA itself violates the Constitution;

- The Commentators' arguments fail because they:

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00090 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.023

- ignore completely two entire lines of well-established Supreme Court cases relating to: (a) the President's "core," "plenary" constitutional authority over foreign intelligence operations; and (b) the separation-of-powers doctrine; and

- overly rely on – and misinterpret – a single case relating to primarily "domestic" actions by a President, in which foreign intelligence operations like those at issue here were not implicated.

- The Commentators' fundamental mistake is the assertion that, if the NSA Program falls into "Zone 3" (where the President's authority is at its "lowest ebb," *though not extinguished*) of Supreme Court Justice Jackson's famous 1952 analysis in *Youngstown Sheet & Tube*, the constitutional analysis ends there and the President is compelled to follow every dictate of FISA;

- Taken to its logical extreme, the Critics' position would fundamentally alter the system of separation of powers and checks and balances created by our Constitution, transforming our governmental system into one in which Congress alone reigns supreme in virtually all spheres of governmental action;

- The better constitutional analysis in areas of shared Executive and Congressional authority, and one more consistent with recent Supreme Court separation-of-powers opinions, and with *Youngstown* itself, balances the relative constitutional authorities of the President and Congress. Even where, in Justice Jackson's terminology, the President's authority is at its "lowest ebb," it obviously is not extinguished, as recognized by the very next words of Justice Jackson's opinion, conceding that the President still can rely "upon his own constitutional powers minus any constitutional powers of Congress;"

- Under this more appropriate analysis, the President's powers over the conduct of foreign intelligence operations appear significantly stronger than those of Congress, since Supreme Court decisions place control of foreign intelligence operations at the "core" of the President's "plenary" foreign affairs powers;

- The conduct of foreign intelligence operations, such as the NSA Program, is a "constitutional function" of the President, and within the President's "central prerogatives," which Congress may not constitutionally impair. Therefore, if FISA is interpreted to prohibit the NSA program, FISA itself violates our Constitution (as narrowly applied to the NSA program);

- The Commentators' assertion that the President, in authorizing the NSA Program, engaged in criminal behavior collapses under the weight of legal advice, based on Supreme Court precedent, propounded by the Clinton Administration as well as other administrations of both political parties, that the President has the authority, if not the

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00091 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.024

duty, to decline to follow portions of statutes reasonably believed to be unconstitutional and, further, that the President may do so without public announcement, except in the time, manner, and form he chooses; and

- Whether FISA is unconstitutional as applied to the NSA Program will turn on facts and circumstances we do not yet know. Assuming the facts as I have in this letter, however, the President could reasonably have concluded that FISA, as applied, would impermissibly impede his ability to carry out his constitutional responsibility to collect foreign intelligence and protect the Nation from attack and, therefore, the President was constitutionally entitled to decline to adhere to FISA's requirements in the narrow circumstances of the NSA Program. In so doing, the President would have, in every sense, acted lawfully and constitutionally.

Detailed discussion, and United States Supreme Court and other legal precedent, supporting the points made above, are contained in Sections II through IV, below.

I. *Introduction*

This analysis sets forth certain Constitutional arguments supported by Supreme Court and other federal court precedent, historical practice, and my first-hand understanding of the interpretation of national security law over at least two administration, that of President Clinton and of President George W. Bush. In order to focus on these important constitutional issues, this letter does not address certain other arguments, including those based on the September 18, 2001 Authorization to Use Military Force ("AUMF"), or on Congress' intent in passing the Foreign Intelligence Surveillance Act of 1978 ("FISA").

Before proceeding, it must be acknowledged that, in the debate over the constitutional separation of powers between the Executive and Congress -- a debate that has raged from the founding of the Nation -- there is a "poverty of really useful and unambiguous authority applicable to concrete problems of executive power as they actually present themselves" as Justice Jackson famously put it.[3] Further, because the full details of the NSA Program are unknown – and may never be known outside of classified hearings given the highly sensitive nature of the methods likely employed – I make certain assumptions for purposes of this letter about the facts, based on publicly reported descriptions as of February 3, 2006, as set out below:

For purposes of this letter, then, I assume the following facts:

- Following the single deadliest attack against civilians on US soil by a foreign enemy (al Qaeda) in our history, facilitated, at least in part, by electronic communications between al Qaeda operatives physically located within the United States and those overseas, the President authorized the NSA to intercept international communications of individuals where there is a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda,

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00092 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.025

without first obtaining an order under FISA;

- The NSA Program targets, for interception of content, communications in which at least one party to the communication is reasonably believed to be physically located overseas, but at least some of this activity falls within FISA's definition of "electronic surveillance;"[4]

- The President reasonably considered the NSA Program an important component of what he had determined, and announced – with Congressional support in the form of an authorizing resolution – to be a global military campaign against al Qaeda and related terrorist organizations; and

- The President, advised by appropriate intelligence and national security law experts, reasonably concluded that the communications targeted by the NSA Program could not be collected in a fashion sufficiently timely to carry out, under the bureaucratically demanding strictures of FISA, his constitutional responsibilities to collect foreign intelligence and protect the Nation from attack.

II. *The Critical Gap in Published Constitutional Analyses of the NSA Program*

Most of the published legal analyses to date examining the constitutionality of the President's authorization of the NSA Program begin and end roughly as follows: [5]

- Congress has certain enumerated constitutional authorities related to electronic surveillance within the United States, and it passed FISA pursuant to those authorities;

- FISA "comprehensively regulates" electronic surveillance for foreign intelligence purposes within the United States; Congress intended FISA to be the "exclusive means" for such electronic surveillance; and FISA criminalizes all other electronic surveillance (with the exception of Title III surveillance for criminal investigations);

- Whatever the President's inherent constitutional authority to conduct warrantless electronic surveillance for foreign intelligence purposes (which numerous federal court decisions have upheld, and even most of the Commentators concede, the President possessed prior to FISA), FISA was intended to fully cabin that authority;

Therefore (and here is where these analyses go fatally off course):

- The Commentators asserting the illegality of the NSA Program conclude that, where Congress has any constitutional role whatsoever in a particular area, and intends to make its mandated procedures "exclusive," the President is *completely foreclosed* from exercising the "core"[6] of his "plenary"[7] constitutional foreign affairs authority -- that is, the collection of foreign intelligence -- except when complying with each and every provision of FISA.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00093 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.026

- These Commentators appear to contend that this is so even if FISA, as applied to the narrow facts and circumstances of the NSA Program, is, itself, unconstitutional. That is, at least some of the Commentators seem to they believe the President commits a crime by declining to execute a law that, itself, violates the United States Constitution.[8]

Such conclusions are unwarranted as a matter of law, unwise and unworkable as a matter of practice, and, most importantly, are themselves constitutionally suspect. Although, of course, "no one is above the law," the United States Constitution is the highest law in our Nation, and statutes inconsistent with the Constitution cannot stand or be enforced by courts.[9]

As Walter Dellinger (today a signatory of the *Cole-Dellinger Letter*,[10] which opines that the NSA Program is illegal), President Clinton's then-Assistant Attorney General for the Office of Legal Counsel (OLC),[11] advised the Clinton Administration in 1994:

> [W]here the President believes that an enactment unconstitutionally limits his powers, he has the authority to . . . *decline to abide by it*, unless he is convinced that the [Supreme] Court would disagree with his assessment.[12]

A. The Commentators' Misreading and Attempted Overextension of Youngstown[13]

In the 1952 case of *Youngstown Sheet & Tube v. Sawyer*, Supreme Court Justice Robert Jackson's concurring opinion famously articulated a three-part analysis for assessing the constitutionality of a President's actions.[14] In so-called "Zone 1," where a President acts pursuant to authorization by Congress (express or implied), the President is in his most powerful constitutional position, because he exercises not only his own constitutional powers, but "all that Congress can delegate."[15] In "Zone 2," where Congress has not spoken in a particular area, the President must rely upon his constitutional powers alone.[16] In Zone 3, where Congress, by statute, has attempted to foreclose or regulate the President's actions, his power is at its "lowest ebb," because he can "rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter."[17]

The Commentators assert that the NSA Program must fall into Zone 3, based on their reading of FISA's exclusivity provision, and their rejection of the Administration's argument that the AUMF is a statutory augmentation of the President's own constitutional powers in the area of foreign intelligence electronic surveillance. The Administration argues that passage of the AUMF places the NSA Program into Justice Jackson's Zone 1 which, if correct, would eliminate the need for the constitutional analysis put forward in this letter, for the NSA Program then would be clearly constitutional without needing to rely on the President's inherent constitutional authority. For purposes of this letter, while acknowledging the legitimacy of the Administration's position, I assume that the NSA Program falls into Justice Jackson's Zone 3.

As noted above, the Commentators assert that, if the NSA Program falls into Zone 3, the constitutional analysis ends, and the President's authorization of the NSA Program must be

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00094 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.027

illegal. Beyond one sentence in *Youngstown* itself, the Commentators cite virtually no judicial authority for this position, however, and my research has identified none.

To the contrary, the Commentators' position is undermined by:

1. Justice Jackson's *Youngstown* opinion itself;
2. The vast difference between the facts and circumstances at issue in *Youngstown*, and those in the current debate;
3. Supreme Court jurisprudence establishing the primary position of the President in foreign affairs and, particularly, in foreign intelligence operations, such as the NSA Program;
4. Decades of Supreme Court and other federal court decisions, as well as Executive Branch legal opinions under both political parties, concerning the constitutional separation of powers between Congress and the Executive; and
5. Longstanding legal precedent establishing a President's authority, if not duty, to decline to execute statutory provisions the President reasonably believes violate our Constitution.

1. *Misreading of Justice Jackson's Opinion*

Some of the Commentators' analysis simply ends with a reference to the statement by Justice Jackson that the President's power is at its "lowest ebb" in Zone 3, moving on to assert the illegality of the NSA Program. Those that cite any legal authority for this position appear to rely solely on Justice Jackson's statement that "[c]ourts can sustain exclusive Presidential control in such a case only by disabling the Congress from acting upon the subject."[18]

I have been unable to find a single Supreme Court case in the more than 50 years since *Youngstown* in which this principle asserted by the Commentators has been used to strike down any President's decision to decline to abide by a part of a statute the President believed violated our Constitution. Furthermore, a moment's reflection on this proposition demonstrates that it could not possibly have been intended to carry the decisional weight the Commentators place on it.

To cite just a few examples of actions that, if the Commentators' arguments were correct, may well have been lawful exercises of Congress' power,:

- Congress could, by virtue of its power to ratify treaties, control negations with foreign governments;[19]

- Congress could, by virtue of it's authority to declare war, prevent a President from using military force to respond to an overseas attack on Americans, a power which Congress itself appears to have conceded it does not have;[20]

- Congress could, by virtue of its authority to make rules for the Army and Navy, completely foreclose the President, as Commander in Chief, from holding courts martial for military

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00095 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.028

personnel;[21] or

- Congress could, by virtue of its power to make and support armies and make all laws necessary and proper to that end, prevent the President from placing U.S. troops under United Nations Command (an action by Congress viewed as an unconstitutional act by Congress, at least in the formal OLC opinion of then-Clinton Administration Assistant Attorney General Dellinger).[22]

In each of these cases, however, as demonstrated by the legal authorities cited in the endnotes, our Courts and/or Executive Branch legal opinions (under both political parties) have rejected such exercises of Congress' power as unconstitutional.

Put another way, the Commentators' position, taken to its logical extreme, would fundamentally alter the system of separation of powers and checks and balances created by our Constitution, transforming our governmental system into one in which Congress alone reigns supreme in virtually all spheres of governmental action. This is likely one reason why, as discussed in Section IV.B., OLC opinions under Presidents of both political parties, are fundamentally incompatible with the Commentators' reading of Justice Jackson's opinion.

Clearly, as the Commentators point out, Congress has multiple constitutionally enumerated powers directly related to the President's Commander-in-Chief power. If the single *Youngstown* sentence on which the Commentators rely were interpreted as the Commentators urge, Mr. Dellinger's advice, to President Clinton, *see, e.g., supra* note 22, as well as many other legal opinions provided to Presidents of both political parties, would be fatally flawed.

The better constitutional analysis in areas of shared Executive and Congressional authority is a more nuanced, balancing approach, taking into account the relative constitutional authorities of the President and Congress.[23] Even where, in Justice Jackson's terminology, the President's authority is at its "lowest ebb," it obviously is not *extinguished*, as recognized by the very next words of Justice Jackson's opinion, which concede that a President may still rely "upon his own constitutional powers minus any constitutional powers of Congress over the matter."[24] This statement would make no sense unless Justice Jackson contemplated circumstances in which powers at this "lowest ebb" still were enough to sustain a President's action (or, put conversely, invalidate Congress' action as unconstitutional).

2. *The Commentators Apply Justice Jackson's Concurrence Beyond Its Reach*[25]

Courts and commentators have long recognized that separation-of-powers conflicts between Congress and the President, such as that underway today with regard to the NSA Program, must be analyzed quite differently in foreign affairs/national security cases than in cases involving principally domestic issues.[26] In primarily foreign affairs/national security cases, much greater deference must be given to the President's authority, and expressions of Congressional will are treated as far less dispositive, than in primarily domestic cases.[27]

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00096 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.029

Even a cursory analysis of *Youngstown* shows that, although the Executive/Congressional conflict at issue in that case unfolded against the backdrop of the Korean War, the issues at stake were far more "domestic" in nature than those involved in the NSA Program. *Youngstown* involved President Truman ordering the seizure and control by the U.S. Government of U.S. steel mills due to the failure of the steel industry and unions to reach a collective bargaining agreement.[28] In striking down President Truman's seizure by Executive Order, the majority in *Youngstown* recited the following powers of Congress:

> It can authorize the taking of private property for public use. It can make laws regulating the relationships between employers and employees, prescribing rules designed to settle labor disputes, and fixing wages and working conditions in certain fields of our economy.[29]

The *Youngstown* majority also relies more generally upon Congress' authority to "make all laws which shall be necessary and proper,"[30] but, tellingly, does *not* rely on Congress' enumerated powers to raise and support an Army or to provide and maintain a Navy. Although Justice Jackson's concurring opinion (one of five in the case) discusses these powers, he couples them with Congress' exclusive power over the "raising of revenues and their appropriation."[31]

Moreover, Justice Jackson himself, noting that Congress could directly "take over war supply," then asked the rhetorical question: "[I]f Congress sees fit to rely on free private enterprise collectively bargaining with free labor for support and maintenance of our armed forces can the Executive . . . seize the facility for operation upon Government-imposed terms?"[32] Justice Jackson, then, saw the *Youngstown* steel seizure as an activity encompassing powers over our domestic economy and labor relations overwhelmingly vested by the Constitution and court decisions in the Congress, albeit with some limited authority in related areas committed to the President.

As discussed in detail in Section III, the *Youngstown* situation stands in stark contrast to the President's foreign intelligence/foreign affairs power at issue in the context of the NSA Program. The Commentators' failure to recognize this fundamental difference between *Youngstown* and the NSA Program weakens, to the point of collapse, the force of their constitutional analysis. Whatever the precise constitutional contours of Congressional and Executive power where regulation of our domestic economy intersects with the supply of our armed forces, even during active hostilities, the vastly greater constitutional power of the President in the field of foreign affairs, national security and, particularly, the conduct of foreign intelligence operations, as discussed below, is clear. Moreover, it is decisive, even assuming, *arguendo*, that the words of FISA place the President at the "lowest ebb" of those powers in this current separation-of-powers conflict with the Congress.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00097 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.030

Despite the implication in the Commentators' writings to the contrary, not every statute passed by Congress can, merely by using words of "exclusivity," completely extinguish the constitutional prerogatives of another co-equal branch of our government. If Congress could do so, we would not need a judicial branch to decide constitutionality/separation-of-powers issues. Congress' word, whether constitutional or not, would simply be final in all cases.

As attractive as that may be to some, it simply is not the constitutional system our framers designed. Rather, although the Commentators' fail to discuss this central tenet of our constitutional system, the actions of all three branches of our government are limited by separation-of-powers principles that have structured our constitutional arrangement since the founding."[46]

As the Supreme Court reminded us in 1996: "Even before the birth of this country, separation of powers was known to be a defense against tyranny . . . . [and] it remains a basic principle of our constitutional scheme that one branch of the Government may not intrude upon the central prerogatives of another. . . ."[47] Similarly, in *William Jefferson Clinton v. Paula Corbin Jones*, a seminal recent separation-of-powers case, the Supreme Court held:

> The doctrine of separation of powers is concerned with the allocation of official power among the three coequal branches of our Government . . . . Thus, for example, the Congress may not exercise . . . the executive power to manage an airport."[48]

In reaffirming this fundamental constitutional principle, and the "unique position in the constitutional scheme" occupied by the President, it is no accident that the Supreme Court -- some 45 years after *Youngstown* -- chose to use the President's foreign affairs authorities as an example of where separation-of-powers, in some cases, must trump authorities of another co-equal branch of government. The Court thus reminded us that the conduct of foreign affairs is "a realm in which the Court has recognized that [i]t would be intolerable that courts, without the relevant information, should review and perhaps nullify actions of the Executive taken on information properly held secret."[49] Interestingly, the original source of this 1997 Supreme Court statement was a previous Supreme Court case that made note of the President's core authority over foreign intelligence activities.[50]

The Supreme Court has provided some guidance for the admittedly difficult task of determining whether particular attempts by one of our three co-equal branches of government to tie the hands of another branch are unconstitutional and, therefore, without legal effect. As recently as 1997, the Supreme Court reaffirmed that one branch of government may not, consistent with our Constitution, "impair another in the performance of its constitutional duties."[51] In *Clinton v. Jones*, the Supreme Court unanimously rejected President Clinton's claim to temporary immunity from any civil legal proceedings against him, which claim was based in significant part on President Clinton's separation-of-powers assertion that his powers were "so vast and important" as to "place limits on the authority of the Federal Judiciary."[52]

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00098 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.031

Although the Court rejected President Clinton's claim of immunity, it unanimously reaffirmed the important place of separation-of-powers analysis in our constitutional system of government. Relying on decades of its own precedent, the Supreme Court's separation-of-powers analysis appeared to turn on the "possibility that the [actions of one co-equal branch of government, in that case, the Federal Judiciary] will curtail the scope of the official powers of the Executive Branch."[53] Put another way, the Supreme Court's test for whether one branch of government has violated our constitutional principle of separation of powers and, therefore, acted unconstitutionally, is whether the action rises "to the level of constitutionally forbidden impairment of the Executive's ability to perform its constitutionally mandated functions."[54]

As discussed in Section III.B, the conduct of foreign intelligence operations is a "constitutional function" of the President, and is within one of the President's "central prerogatives," which Congress may not constitutionally impair. Recognition of this may have led the Congress that passed FISA to state, even as it was passing the law, that:

> The conferees agree that the establishment by this act of exclusive means by which the President may conduct electronic surveillance *does not foreclose a different decision by the Supreme Court*. The intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the [*Youngstown*] case."[55]

Surprisingly, the Commentators generally either ignore, or pay only brief lip service to, this extraordinary admission accompanying the original passage of FISA. This statement, by the Congress that passed FISA, is significant for several reasons. First, it acknowledges that Congress itself had some doubt about the constitutionality of FISA's attempt to completely control the President's authority to conduct electronic surveillance for foreign intelligence purposes. Second, it suggests that Congress understood that, even within Justice Jackson's Zone 3, there are limits to the degree to which Congress may constitutionally restrict the President in the area of foreign intelligence collection.

Finally, the statement by the Congress enacting FISA indicates that Congress specifically contemplated that the degree to which FISA might constitutionally tie the President's hands could one day reach the Supreme Court. This makes sense if, but only if, Congress contemplated that then-President Carter, or a future President, might be required to act outside the FISA statute, exercising the very inherent authority that Congress was attempting to limit.

As discussed above, then, the weight of Supreme Court authority, as well as more than 200 years of Executive practice, provide ample support for the view that, if construed to foreclose the type of NSA foreign intelligence collection assumed herein, FISA is unconstitutional as applied to the NSA Program to the extent it impermissibly impedes the President's ability to carry out his constitutional responsibilities to collect foreign intelligence and protect our Nation from attack.

Just as the *Youngstown* analysis does not end the inquiry, however, neither does a conclusion of unconstitutionality. The question then becomes, what is a President permitted or compelled to do once reasonably reaching such a conclusion?

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00099 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.032

B. The President's Constitutional Authority to Decline to Follow Unconstitutional Statutes

The Commentators charge that the President, in authorizing the NSA Program, acted illegally because, Congress having spoken definitively through FISA, the President had no lawful option except to follow the statute to the letter, even if FISA itself was in violation of our Constitution. This conclusion, while perhaps politically appealing in the short term, defies decades of Supreme Court and other legal precedent, as well as Executive Branch legal opinions by Administrations of both political parties, holding that Presidents have the constitutional prerogative – if not the constitutional duty – to decline to follow provisions of statutes they reasonably believe to be unconstitutional.

As noted above, one of the most thoughtful and persuasive enunciations of this conclusion was drafted, interestingly enough, by one of the signatories of the aforementioned Cole-Dellinger letter, sharply critical of the President's authorization of the NSA Program. Then-Assistant Attorney General Walter Dellinger advised President Clinton's counsel of the "general proposition that I believe to be uncontroversial: there are circumstances in which the President may appropriately decline to enforce a statute that he views as unconstitutional."[56]

Dellinger cited "significant judicial approval" of this proposition, including:

> the Court's decision in *Myers v. United States*, 272 U.S. 52 (1926). There the Court sustained the President's view that the statute at issue was unconstitutional without any member of the Court suggesting that the President had acted improperly in refusing to abide by the statute. More recently, in *Freytag v. Commissioner*, 501 U.S. 868 (1991), all four of the Justices who addressed the issue agreed that the President has "the power to veto encroaching laws . . . *or even to disregard them when they are unconstitutional*." *Id.* at 906 (Scalia, J., concurring); *see also Youngstown Sheet & Tube v. Sawyer*, 343 U.S. 579, 635-38 (1952) (Jackson, J., concurring) (recognizing existence of President's authority to act contrary to a statutory command).[57]

Dellinger further opined that:

> consistent and substantial executive practice also confirms this general proposition. Opinions dating to at least 1860 assert the President's authority to decline to effectuate enactments that the President views as unconstitutional. *See, e.g., Memorial of Captain Meigs*, 9 Op. Att'y Gen. 462, 469-70 (1860) (asserting that the President need not enforce a statute purporting to appoint an officer)."[58]

After wisely cautioning that the President should decline to enforce a statute he or she considers unconstitutional only where he or she believes the Supreme Court would agree, and then only in rare cases, Dellinger advised President Clinton, through his counsel, as follows, at least

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00100 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.033

implicitly suggesting that the President has a constitutional duty to decline to execute unconstitutional statutory provisions:

> The President has *enhanced responsibility to resist unconstitutional provisions that encroach upon the constitutional powers of the Presidency.* Where the President believes that an enactment unconstitutionally limits his powers, he has the authority to defend his office and decline to abide by it, unless he is convinced that the Court would disagree with his assessment. . . . If the President does not challenge such provisions (*i.e.,* by refusing to execute them), there often will be no occasion for judicial consideration of their constitutionality; a policy of consistent Presidential enforcement of statutes limiting his power thus would deny the Supreme Court the opportunity to review the limitations and thereby would allow for unconstitutional restrictions on the President's authority. [59]

Finally, consistent with the view of Presidential authority in foreign and military affairs discussed in prior sections of this letter, Dellinger advised that a President's responsibility to decline to execute unconstitutional statutory provisions is:

> usually true, for example, of provisions limiting the President's authority as Commander in Chief. Where it is not possible to construe such provisions constitutionally, the President has the authority to act on his understanding of the Constitution.[60]

Some have asserted that the President acted criminally by failing either to seek legislative relief from, or publicly declare his belief in, the unconstitutionality of, FISA, as applied. Quite to the contrary, as then-Assistant Attorney General Dellinger advised President Clinton, through his counsel, the President can not only decline to enforce an unconstitutional provision without any public statement whatsoever, but he could even do so with regard to a statute he himself signed into law. Because this advice is so relevant to the charges now leveled against the President, I quote Mr. Dellinger's 1994 advice to President Clinton's counsel at some length:

> The fact that a sitting President signed the statute in question does not change this analysis. The text of the Constitution offers no basis for distinguishing bills based on who signed them; there is no constitutional analogue to the principles of waiver and estoppel. Moreover, every President since Eisenhower has issued signing statements in which he stated that he would refuse to execute unconstitutional provisions. . . . As we noted in our memorandum on Presidential signing statements, the President "may properly *announce* to Congress and to the public that he will not enforce a provision of an enactment he is signing. If so, then a signing statement that challenges what the President determines to be an unconstitutional encroachment on his power, or that announces the President's unwillingness to enforce (or willingness to litigate) such a provision, can be a valid and reasonable exercise of Presidential authority." . . . . (*Of course, the President is not obligated to announce his reservations in a signing statement; he can convey his views in the time, manner, and form of his choosing.*) Finally, the Supreme Court recognized this practice in *INS v. Chadha*, . . . [stating]: *"it is not uncommon for Presidents to approve legislation containing parts which are objectionable on constitutional grounds"* and then

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00101 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.034

> cited the example of President Franklin Roosevelt's memorandum to Attorney General Jackson, in which he indicated his intention not to implement an unconstitutional provision in a statute that he had just signed. . . . These sources suggest that the President's signing of a bill does not affect his authority to decline to enforce constitutionally objectionable provisions thereof.[61]

Though the title of this opinion diplomatically describes the President's constitutional authority as one to "decline to execute" unconstitutional statutes, it is clear, from this and other OLC opinions, that the intent was to confirm the President's authority, in rare cases, to act in contravention of provisions reasonably believed unconstitutionally to intrude on the President's constitutional responsibilities and authorities.

To cite one particularly pertinent example that this constitutional authority empowers the President not only to refuse to execute a statute requiring some affirmative act on the President's part, but also to act inconsistently with a statutory requirement or prohibition, is a 2000 OLC opinion for the Clinton Administration, ironically concerning electronic surveillance exclusively regulated by Congress. That opinion advised that "extraordinary circumstances" could arise in which "the President's constitutional powers permit disclosure of [criminal wiretap] . . . information to the intelligence community *notwithstanding the restrictions of Title III*."[62] In other words, President Clinton's Administration was advised, correctly in my view, that the President could act *in direct contravention of a criminal statute*, because limiting "the access of the President and his aides to information critical to national security or foreign relations . . . would be unconstitutional as applied in those circumstances."[63]

This OLC Opinion, prepared for President Clinton's Office of Intelligence Policy and Review by then-Assistant Attorney General Randolph D. Moss, advised that the President could disregard statutory restrictions on sharing criminal wiretap information with intelligence officers, notwithstanding that the statute at issue carried criminal penalties. OLC advised that:

> [I]n extraordinary circumstances electronic surveillance conducted pursuant to Title III may yield information of such importance to national security or foreign relations that the President's constitutional powers will permit disclosure of the information to the intelligence community notwithstanding the restrictions of Title III. . . . [T]he Constitution vests the President with responsibility over all matters within the executive branch that bear on national defense and foreign affairs, including, where necessary, *the collection and dissemination of national security information*. Because "[i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation," *Haig [v. Agee]*, 453 U.S. at 307 (quoting *Aptheker v. Secretary of State*, 378 U.S. 500, 509 (1964)), the President has a powerful claim, under the Constitution, to receive information critical to the national security or foreign relations and to authorize its disclosure to the intelligence community. Where the President's authority concerning national security or foreign relations is in tension with a statutory rather than a constitutional rule, the statute cannot displace the President's constitutional

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00102 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.035

> authority and should be read to be "*subject to an implied exception* in deference to such Presidential powers." *Rainbow Navigation, Inc. v. Department of the Navy*, 783 F.2d 1072, 1078 (D.C. Cir. 1986) (Scalia, J.). *We believe that, if Title III limited the access of the President and his aides to information critical to national security or foreign relations, it would be unconstitutional as applied in those circumstances.*[64]

Of course, even if FISA, as applied, is unconstitutional and, therefore, the President has full constitutional authority to decline to execute FISA as such, the NSA Program still must comport with the reasonableness requirements of the Fourth Amendment. Whether it does will depend completely on the precise facts and circumstances of how the program actually is being executed, and we simply do know enough yet (and the public may never know enough) about the program to reach a definitive judgment on that question. Based on what has been said publicly, however, it appears likely that the Supreme Court would find the NSA Program "reasonable," in light of: (a) the magnitude of the threat to our Nation, and the nature of the targets of the NSA Program; (b) the use of "minimization" procedures;" and (c) initial internal review by multiple legal officials, along with regular legal -- and, apparently, Presidential -- review of the program.

V. *Application of These Principles to the Assumed Facts of NSA Program*

I do not assert in this letter that FISA is unconstitutional in all, or even most, respects. Whether or not it is unconstitutional *as applied* to the NSA Program also will turn on facts and circumstances we do not yet know. Assuming the facts as I have in this letter, however, the President could have reasonably concluded that FISA, as applied, would impermissibly impede his ability to carry out his constitutional responsibility to collect foreign intelligence and protect the Nation from attack.

It is difficult to predict accurately what the Supreme Court would do, particularly without knowing the facts of a particular case, or whether the Court would decline to intervene at all in what it might judge to be a separation-of-powers dispute over the NSA Program best left to the two "political" branches of government. That said, based on previous separation-of-powers decisions and Fourth Amendment decisions concerning "reasonability," I would expect the key factors to be:

- Whether the President, advised by intelligence professionals, reasonably concluded that the information collected by the NSA Program was important to identifying, and preventing, terrorist activities directed against the United States, here or abroad;

- If so, whether abiding by all provisions of FISA would negate or significantly impede the President's ability to gather such information in a sufficiently timely way to thwart such activities; and

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00103 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.036

- Whether the President reasonably concluded there was no reasonable alternative to the NSA Program, consistent with FISA's requirements, available to the Executive Branch.

If the President could reasonably answer all three of these questions in the affirmative, I believe the President would have been justified in anticipating that the Supreme Court would find the NSA Program constitutional or, put conversely, an interpretation of FISA foreclosing the NSA Program unconstitutional. Armed with that reasonable anticipation of the Supreme Court's ultimate decision, the President would have been constitutionally empowered, if not obligated, to decline to carry out FISA's requirements. As legal advice given to President Clinton indicates, the President was not required to make any announcement of his decision, except in the time, manner, and form of his choosing.[65] In declining to carry out FISA's requirements under these circumstances, far from acting criminally, the President would have, in every sense, acted lawfully and constitutionally.

It is my hope that the perspectives raised, and authorities cited, in this letter will assist the Congress in the separation-of-powers debate already underway.[66]

Sincerely,

H. Bryan Cunningham

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00104 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.037

[1] *See curriculum vitae*, attached hereto. I currently practice information and homeland security law in Denver, Colorado. www.morgancunningham.net.

[2] I note that I had no knowledge of the NSA program while in government, and have received no classified information about it.

[3] *Youngstown Sheet & Tube Co. v. Sawyer,* [3] 343 U.S. 579, 634 (1952). Today, there is a good deal more Supreme Court law, and Executive Branch interpretation of it, than was available to Justice Jackson in 1952, the vast majority of it supportive of the views articulated in this letter.

[4] Although at least one press report has suggested that some small percentage of the electronic surveillance under the NSA Program may have involved communications where both parties were physically located in the United States, to my knowledge, there has been no allegation that any such interceptions were deliberate, but only that they were done, if at all, mistakenly.

[5] I take no position in this letter on the following issues widely discussed to date: (a) the degree to which FISA foreclosed reliance on statutes other than FISA and Title III of the Omnibus Crime Control Act and Safe Streets Act of 1968 ("Title III") to conduct the NSA Program; (b) whether the AUMF in any way augmented to conduce the NSA Program or otherwise altered, FISA; (c) the general scope of the constitutional powers and responsibilities of the President as Commander-in-Chief versus Congress under its enumerated authorities; or (d) the reasonableness of the NSA Program under the Fourth Amendment. While I have views on each of these issues, I believe that they have been sufficiently discussed, on both sides of each issue and that, in contrast to the issues discussed in this letter, I have little to add to the debate.

[6] *See Webster v. Doe*, 486 U.S. 592, 605-06 (1988) (O'Connor, J. concurring).

[7] *See United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936).

[8] *See, e.g.,* January 9, 2006 *Letter to Members of Congress*, from 14 law professors and others currently in private sector, including Curtis A. Bradley, David Cole, and Walter Dellinger, former Assistant Attorney General, Office of Legal Counsel to President Clinton ("the Cole-Dellinger Letter"), ("Where Congress has . . . [regulated electronic surveillance] the President can act in contravention of statute only if his authority is *exclusive*, and not subject to the check of statutory regulation." at 2); January 5, 2006 Congressional Research Service Memorandum entitled *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information* ("CRS Surveillance Memo"); January 3, 2006 *Letter from Jeffrey H. Smith to Members of the House Permanent Select Committee on Intelligence* ("Smith Letter") ("[Because] Congress has the authority to 'make rules for the Government and regulation of the land and naval forces,' [and other enumerated constitutional powers], [and because] Congress intended FISA to be the exclusive means by which electronic surveillance of U.S. persons within the United States may be conducted, . . . the President lacks the residual constitutional authority to conduct [it]." at 10 (emphasis added)) available at http://www.rawstory.com/exclusives/nsaspymemo.pdf; January 26, 2006 Internet posting by Peter P. Swire, entitled *Legal FAQs on NSA Wiretaps* ("Swire Memorandum") ("In short, it is a crime to conduct wiretaps in the United States, of U.S. citizens, unless there is a statutory basis for doing so. There was no statutory basis [for the NSA Program]." at 2) available at http://www.americanprogress.org/site/pp.asp?c=biJRJ8OVF&b=1389573; and *A Legal Analysis of the NSA Warrantless Surveillance Program*, Morton H. Halperin and Jerry Berman, January 31, 2006 ("Halperin/Berman Letter") ("[The Administration's] claim—that the program is legal because the President has inherent authority to authorize warrantless wiretaps—might have had some plausibility if Congress had not acted so decisively to prohibit warrantless surveillance in the United States when it enacted FISA." at 5), available at http://cdt.org/security/nsa/20060131halperinberman.pdf. I refer to these published legal analyses collectively as "the Commentators". There is, of course, some variation between the articulation of these fundamental points between and among the Commentators quoted here, as well as in the degree of certainty and stridency (i.e., accusing the President of deliberate criminal behavior) expressed in each of the individual sources cited. Except as directly quoted, I do not mean to ascribe my specific formulation to any particular source cited. However, I believe the immediately preceding summary to be a fair representation of the general thrust of the Commentators' argument.

[9] Not all who have previously published legal analyses believe the President's actions violated the Constitution or were illegal, and the critiques do not break down easily along partisan lines. *See, e.g.*, December 21, 2005 editorial by former Associate Attorney General to President Clinton John Schmidt asserting the legality, and consistency with

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00105 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.038

past practice in other Administrations, of the NSA Program. Available at http://www.weeklystandard.com/weblogs/TWSFP/2005/12/clinton_associate_attorney_gen.html.

[10] *supra* note 8.

[11] Opinions of the DOJ Office of Legal Counsel are widely recognized as legally binding across the Executive Branch. *See, e.g.,* Randolph D. Moss, *Executive Branch Legal Interpretation: A Perspective from the Office of Legal Counsel*, 52 Admin. L. Rev. 1303, 1318 (Fall 2000) ("In the overwhelming majority of cases, when the views of the Attorney General or the Office of Legal Counsel are sought, all understand that those views will conclusively resolve the legal question presented, short of subsequent judicial review)".

[12] Reaffirming this constitutional authority apparently was sufficiently important to President Clinton's Administration that Assistant Attorney General Dellinger wrote an entire opinion about it, even though the opinion does not identify any particular statute at issue at the time. *Presidential Authority to Decline to Execute Unconstitutional Statutes*, 4A U.S. Op. OLC 55, November 2, 1994. The cited quote is from page 2 of that opinion (emphasis added).

[13] I personally have worked with or for a number of the lawyers I describe in note 8 as "the Commentators." Those whom I know are honorable individuals, and talented and experienced lawyers, and, no doubt, are articulating the law as they honestly believe it to be. I take no issue with any of them personally. I simply believe that, in the case of the NSA Program, their constitutional analysis is incomplete and flawed, and I feel it important to make Congress aware of additional, relevant, constitutional and legal authority.

[14] *Supra* note 3, at 635-38.

[15] *Id* at 635.

[16] *Id.* at 637.

[17] *Id.*

[18] *Id.* at 637-38.

[19] Such a result has been flatly rejected by a number of federal court decisions, *e.g., Earth Island Inst. v. Christopher*, 6 F.3d 648, 652-53 (citing *Curtiss-Wright* and holding: "The district court correctly ruled that the section 609(a) claims relate to 'the foreign affairs function, which rests within the exclusive province of the Executive Branch under Article II, section 2 of the United States Constitution.' The statute's requirement that the Executive initiate discussions with foreign nations violates the separation of powers, and this court cannot enforce it").

[20] 50 U.S.C. § 1541(c) (recognizing, in the War Powers Act, the President's constitutional authority to respond militarily, without statutory authorization, to a "national emergency created by attack upon the United States, its territories or possessions, or its armed forces"); In any event, "[t]he Executive Branch has traditionally taken the position that the President's power to deploy armed forces into situations of actual or indicated hostilities is not restricted to the three categories specifically marked out by the [War Powers] Resolution. *Proposed Deployment of United States Armed Forces Into Bosnia*, 19 U.S. Op. OLC 327 (1995), at 7 (citing *Overview of the War Powers Resolution*, 8 Op. OLC 271, 274-75 (1984); *War Powers: A Test of Compliance: Hearings Before the Subcomm. on International Security and Scientific Affairs of the House Comm. on International Relations*, 94th Cong., 1st Sess. 90 (1975) (statement of Monroe Leigh, Legal Adviser, Department of State)).

[21] "The power of the executive to establish rules and regulations for the government of the army, is undoubted." *United States v. Eliason,* 41 U.S. 291, 301 (1842) (cited with approval in *Loving v. United States, infra* note 47 at 767 ("Congress . . . exercises a power of precedence over, not exclusion of, Executive authority").

[22] *Placing of United States Armed Forces Under United Nations Operational or Tactical Control*, 20 U.S. Op. OLC 182, *2 (1996), 1996 WL 942457.

[23] This type of more nuanced, balancing approach was explicitly endorsed, as a description of Supreme Court separation-of-powers analysis, by Justice Kennedy's concurring opinion in a 1989 separation-of-powers case. In *Public Citizen v. Department of Justice*, Justice Kennedy, citing a number of Supreme Court cases decided well after *Youngstown*, opined: "In some of our more recent cases involving the powers and prerogatives of the President, we have employed something of a balancing approach, asking whether the statute at issue prevents the President 'from accomplishing [his] constitutionally assigned functions' . . . . and whether the extent of the intrusion on the President's powers 'is justified by an overriding need to promote objectives within the constitutional authority of Congress." 491 U.S. 440, 484 (1989) (citations omitted).

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00106 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.039

[24] *Youngstown, supra* note 3, at 637.
[25] Influential as Justice Jackson's opinion has been in helping judges make sense out of complex constitutional questions, it was not the majority opinion in *Youngstown* and, as such, it's effect as binding precedent is not as great as it might be. The Supreme Court, in 1981, did cite *Youngstown* approvingly in a majority opinion, enhancing its status. The Court there, however, in *Dames & Moore v. Regan*, only quoted the part of Justice Jackson's analysis discussing Zone 1. It is unclear, therefore, how much of the analysis is binding. 453 U.S. 654, 678 (1981).
[26] *See, e g., United States v. Brown,* in which the Court of Appeals for the Fifth Circuit, in uphonding the President's inherent constitutional authority to order warrantless foreign intelligence wiretaps, articulated the longstanding constitutional principle that "[r]estrictions upon the President's power which are appropriate in cases of domestic security become artificial in the context of the international sphere." 484 F.2d 418, 426 (5th Cir. 1973).
[27] *See, e.g.*, infra note 42, at 540-41 ("[t]he great bulk of the substantive powers wielded by the executive branch in the domestic arena stems from acts of Congress, and as long as Congress refrains from interfering with the President's constitutional duties of appointment and supervision it has substantial freedom to grant, withhold, and condition domestic authority to the executive. Other than issuing pardons and making state of the union addresses, the President can do very little domestically without congressional authorization. In the areas of foreign affairs and national security, by contrast, constitutional text and structure vest the President with substantive constitutional authority not dependent on congressional enactments, while Congress itself, of course, possesses a variety of relevant powers. When separation of powers questions arise in these areas, therefore, their resolution requires the interpreter to give due weight and proper respect to executive and legislative powers of equal constitutional dignity").
[28] *Youngstown, supra* note 3, at 582-84.
[29] *Id.* at 588.
[30] *Id.*
[31] *Id.* at 643 (though Justice Jackson notes also Congress' power to raise and support armies and establish and maintain a Navy, his is not the majority opinion in the case and, thus, not controlling on this point).
[32] *Id.*
[33] Admittedly, treating the Commander in Chief and foreign affairs powers as completely separate authorities would be inaccurate and artificial. Any serious assessment of the President's constitutional authority to authorize the NSA Program, however, must include an understanding of the foreign affairs power, and how the Supreme Court and Administrations of both political parties, over decades, have viewed that power, and Congressional attempts to regulate its use.
[34] *U.S. Constitution,* art. II, section 1, clause 8.
[35] Indeed, the founders of our republic specifically recognized the primary position of the President in the field of foreign affairs. For an excellent discussion of this history, *see* Powell, H. Jefferson, *The Founders and the President's Authority over Foreign Affairs*. William & Mary Law Review, Vol. 40, pp. 1471-1537 (May 1999).
[36] 22 U.S. Op. Atty. Gen. 13, 25-26, *Foreign Cables*, (1898) (citing, *inter alia, Cunningham v. Neagle*, 135 U.S. 1 (1890)) (emphasis added).
[37] 484 US 518, 527, 530 (1988).
[38] 339 U.S. 763, 789 (1950) (emphasis added).
[39] 299 U.S. 304, 320 (1936) (emphasis added)
[40] *Egan, supra* note 37 at 527, 530.
[41] *Supra* note 26 (emphasis added) (citations omitted). The Commentators argue that the numerous federal appeals court decisions prior to the passage of FISA reiterating the President's inherent constitutional authority to authorize warrantless electronic surveillance for foreign intelligence/national security purposes are not dispositive today because of the intervening passage of FISA. As conceded by the Congressional Research Service in its memorandum expressing doubt about the legality of the NSA Program, however, because "the [Foreign Intelligence Surveillance] Court of Review is a court of appeals and is the highest court with express authority over FISA to address the issue, its reference to inherent constitutional authority for the President to conduct warrantless foreign intelligence surveillance might be interpreted to carry great weight." *CRS Surveillance Memo, supra* note 8, at 30. The FISA Court of Review decision was issued in 2002, more than 20 years after the passage of FISA and is, of itself, strongly supportive of the constitutionality (and, therefore, legality) of the NSA Program. Whatever the merit of the Commentators' position on the relevance of pre-FISA court of appeals decisions regarding the issue of the

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00107 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.040

legality of warrantless electronic surveillance for foreign intelligence purposes, however, neither the passage of FISA, nor any other intervening event, undermines the authority of pre-FISA court of appeals decisions on the Presidents foreign affairs and foreign intelligence authorities generally.

[42] Particularly notable in this area is the body of work of Professor H. Jefferson Powell of Duke University Law School. While I do not claim to know whether Professor Powell would agree with any views expressed in this letter, I am indebted, for much of the legal analysis presented herein, to Professor Powell's exhaustive 1999 article *The President's Authority Over Foreign Affairs: An Executive Branch Perspective,* 67 Geo. Wash. L. Rev. 527. In addition to the exhaustive research that underlies it, Professor Powell's article is additionally interesting due to his previous government service. Professor Powell served in senior legal positions under President Clinton, as Principal Deputy Solicitor General from July 1996 through September 1996, and as Deputy Assistant Attorney General in the Office of Legal Counsel from June 1993 through June 1994, and January 1996 through September 1996.

[43] *Webster v. Doe*, *supra* note 6, 605-06 (emphasis added) (*citing* prior Supreme Court decisions in *United States v Curtiss-Wright Export Corp.*,; *Department of Navy v. Egan*,; and *Totten v. United States*, 92 U.S. 105 (1876)).

[44] To be sure, what Professor Powell has called the "Executive Branch Perspective" concerning the President's constitutional foreign affairs authority is not universally shared. According to Professor Powell, as of 1999, "the conventional wisdom in recent scholarship" rejected "any interpretation of the Constitution that accords the President primary constitutional responsibility for the formulation of United States foreign policy. Powell, *supra* note 35 at 1 (Professor Powell cites several examples of what he calls the "congressional primacy" view in his William and Mary Law Review article, *supra* note 35). The problem, as Professor Powell notes, for those espousing this "congressional-primacy" view of constitutional foreign affairs authority, is that, to do so requires one to "repudiate or distinguish away most of what the Supreme Court appears to have said on the subject. *Id.*

[45] For important elements of the separation-of-powers analysis in this letter, I am indebted to the excellent work of David S. Kris,, a former senior Department of Justice attorney in the Administrations of Presidents Clinton and George W. Bush, though I do not know whether he would agree with any of the views expressed herein.

[46] *Clinton v. Jones*, 520 U.S. 681, 697 (1997).

[47] *Loving v. United States,* 517 U.S. 748, 757 (1996).

[48] *Supra* note 46, at 699-700.

[49] *Id.* at 699.

[50] *Chicago & Southern Air Lines, Inc. v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1947) The Supreme Court, in *Clinton v. Jones*, directly cited *Nixon v. Fitzgerald*, 457 U.S. 731, 750 (1982). Decades after *Youngstown*, this same Supreme Court decision – *Chicago & Southern Air Lines* – was cited by one of the several federal courts of appeals to uphold the President's inherent constitutional authority to order warrantless electronic surveillance for foreign intelligence purposes. *United States v. Brown*, *supra* note 26, at 426 (relying in part on *Chicago & Southern Airlines*, the court held that "because of the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs, we reaffirm . . . that the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence").

[51] *Clinton v, Jones*, *supra note* 46, at 701.

[52] *Id.* at 697-98 (I do not by any means suggest here, as President Clinton's counsel seemed to in *Clinton v. Jones*, that any President is temporarily "immune" from the actions of a co-equal branch of government. Rather, as discussed below, I believe our Constitution requires that, when one branch of government unconstitutionally encroaches on another, the other branch is constitutionally empowered to resist such encroachment).

[53] *Id.* at 701.

[54] *Id.* at 702.

[55] *H R. Conf.Rep.No. 95-1720*, at 35, *reprinted in* U.S.C.C.A.N., 4048, 4064.

[56] *Supra* note 12.

[57] *Id.* (emphasis added).

[58] *Id.*

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00108 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.041

[59] *Id.* at 2 (emphasis added) (the opinion went on to say that "[s]ome legislative encroachments on executive authority, however, will not be justiciable or are for other reasons unlikely to be resolved in court. If resolution in the courts is unlikely and the President cannot look to a judicial determination, he must shoulder the responsibility of protecting the constitutional role of the presidency").

[60] *Id.* at 2.
[61] *Id.* at 3-4 (emphasis added) (citations omitted). To conclude that a President is constitutionally permitted not to seek court approval for an activity where Congress has directed that he do so, or to not discuss publicly a decision to decline to execute an unconstitutional statute does not, of course, suggest that these are the best course of action in any particular case. Generally speaking, I believe that the greater the involvement of all three co-equal branches of government, and awareness by the public, of significant national security decisions, the better. Without knowing all the operational and security considerations involved with the NSA Program, it is impossible to say what the best course of action would have been in this case. In any event, the purpose of this letter is neither to condemn or endorse how the NSA Program has been handled, but only to bring to the debate additional constitutional and legal perspective.
[62] *Infra.* note 64.
[63] *Id.* Much has been made in public discussions about the NSA Program about the criminal penalties for violations of FISA, with some even suggesting current government officials have committed criminal acts. In that context, it is worth noting that Title III, which President Clinton was advised he could disregard as unconstitutional if applied in a particular way, carries precisely the same criminal penalty – five years' imprisonment – as FISA. *Compare* 18 U.S.C. § 2511 with 50 U.S.C. § 1809.

[64] *Sharing Title III Electronic Surveillance Material With the Intelligence* Community, 2000 WL 33716983 (OLC), October 17, 2000, at 9 (emphasis added) (citing *Rainbow Navigation Inc. v. Department of the Navy*, 783 F.2d 1072, 1078 (D.C. Cir. 1986).

[65] The bipartisan leadership of both houses of Congress, as well as the bipartisan leadership of both Congressional intelligence oversight committees, agree that they were briefed repeatedly by the Administration on the NSA Program, though there is, based on media reports, some disagreement about the scope and effect of those briefings. Based on media reports, succeeding Chief Judges of the Foreign Intelligence Surveillance Court also were briefed about the NSA Program.

[66] I am indebted to three exceptional lawyers, Diane Lewis Waters, Esq., Amanda M. Hubbard, Esq., Fulbright Scholar, Norwegian Research Center for Computers and Law, and Andrew C. McCarthy, Senior Fellow, Foundation for the Defense of Democracies for their insight and long hours of review and editing assistance. The views expressed herein, as well as any errors, are mine alone.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00109 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.042

cc:

The Hon. Bill Frist
Majority Leader
United States Senate
Washington, D.C. 20510

The Hon. Harry Reid
Minority Leader
United States Senate
Washington, D.C. 20510

The Hon. J. Dennis Hastert
Speaker
U.S. House of Representatives
Washington, DC 20515

The Hon. Nancy Pelosi
Minority Leader
U.S. House of Representatives
Washington, DC 20515

The Hon. F. James Sensenbrenner, Jr.
Chairman
Judiciary Committee
U.S. House of Representatives
Washington, DC 20515

The Hon. John Conyers
Ranking Minority Member
Judiciary Committee
U.S. House of Representatives
Washington, DC 20515

The Hon. Pat Roberts
Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

The Hon. John D. Rockefeller, IV
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

The Hon. Peter Hoekstra
Chairman
Permanent Select Committee
on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

The Hon. Jane Harman
Ranking Minority Member
Permanent Select Committee
on Intelligence
U.S. House of Representatives
Washington, D.C. 20515

The Hon. Alberto R. Gonzales
Attorney General of the United States
Main Justice Building
950 Pennsylvania Ave., N.W. 20530

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00110 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.043

August 28, 2008

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

The Honorable Patrick J. Leahy
Chairman
Senate Judiciary Committee
224 Dirksen Senate Office Building
Washington DC 20510

Dear Chairman Leahy:

On behalf of the Center for Democracy & Technology, I am pleased to submit these answers to follow-up questions that Senators submitted for the record after the Committee's September 25, 2007 hearing, "Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance National Security?"

Questions Submitted by Chairman Patrick Leahy

1. The Administration argues that the changes they sought with the Protect America Act are consistent with the original intent of Congress when it passed FISA in 1978 because FISA was intended to permit interception of all communications of Americans with persons abroad as long as individuals in the U.S. were not targets. They base this on the fact that FISA permitted the interception of all international radio communications, which, they say, carried almost all of the international calls at that time.

   Put aside whether this argument is factually correct. Should we be relying in our current discussion on the policy judgments of the Congress in 1978 about the need to protect international calls? With the enormous increase in Americans' international calls since 1978 as well as the advent of the Internet, email, and other advances in communications technology, would the intent of Congress in 1978 necessarily lead to the same judgment about protections for international communications?

Answer: The intent of Congress in 1978 with respect to one technology or another is not the only factor to consider in ensuring that FISA continues to adequately balance the twin goals of enhancing national security and protecting civil liberties. The Administration itself has argued on many occasions that it is appropriate to amend the Act in ways that depart from Congress' original intent, in order to respond to the changing threat or to changes in communications and surveillance technology.

Specifically with respect to the current debate, it is clear that, in the 30 years since FISA was first adopted, there have been fundamental changes in the extent to which ordinary

53358.044

Americans engage in international communications. When FISA was first enacted, an international telephone call was an expensive rarity for the ordinary person. Now, many ordinary Americans have regular telephone or email communication with relatives and business partners abroad. The interests of these Americans require stronger—not weaker—standards for government interception, closer oversight, new mechanisms for minimization, and limits on retention of inadvertently intercepted communications. Given the global nature of the American economy, widespread reliance on the Internet, and the huge growth in the volume of international communications traffic on the part of ordinary Americans, the vacuum cleaner technology that Congress may have allowed the NSA to apply to radio communications in 1978 is no longer inappropriate, for wire or radio technologies, when aimed at international communications where an American may be on one end of the communication.

2. In response to criticisms that the PAA allows the government to intercept the communications of Americans as much or for as long as it wants as long as those Americans are not targets, the Administration argues that they have no incentive to conduct "reverse targeting." They say that if they are interested in a person in the United States they will want to get a warrant so that they can intercept all of that person's calls.

Does this response satisfy you?

Answer: This response is not satisfactory because reverse targeting is not the main concern. Rather, given the focus of the debate on foreign-to-domestic communications, the main concern is that, even when the government is targeting a non-US person overseas, some of the communications that the government intercepts will be between the targeted person overseas and someone in the US. Indeed, under the Administration's own description of the issue, there will likely be in some cases an American citizen on the other end of the communications that will be intercepted. In our view, this non-targeted party has privacy interests that need some protection. Surely, the government intends to listen to both ends of the conversation and to disseminate anything that might seem to be foreign intelligence about the person in the United States, thus putting that American at risk of misinterpretation or misuse of that information. The minimization rules alone do not provide adequate protection.

Question Submitted by Ranking Member Arlen Specter

> Your written testimony states: "a communications service provider should not have to guess whether cooperation with an apparently illegal request will be excused." Would your analysis of the arguments for retroactive immunity change if the requests received by communications carriers were not "apparently illegal"? Would it be different, for example, if the carriers received a certification of the program's legality?

Answer: Our analysis would not change if carriers received a certification of the program's legality, unless the certification had been issued by the Attorney General in compliance with the statutory certification provisions of 50 U.S.C. §1802 or 18 U.S.C. §2511(2)(a)(ii)(B).

Prior to the enactment of FISA, government officials had engaged in warrantless electronic surveillance, and carriers had assisted with such surveillance, based upon certifications or other claims by the President and others that such surveillance was legal. However, the Supreme Court had never decided whether those claims of legality were correct, leaving the conduct of important intelligence activities without a "secure framework," as this Committee stated in 1977. One of the primary purposes of FISA was precisely to moot the debate over questions of when warrantless surveillance was legal or illegal, saving both intelligence agency employees and the corporate officers of telecommunications providers from having to rely on legal opinions of the Executive Branch. As the House Intelligence Committee said in its report on FISA, "Thus, even if the President has the inherent authority in the absence of legislation to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the conduct of such surveillance by legislating a reasonable procedure, which then becomes the exclusive means by which such surveillance may be conducted." House Report 95-1283, Pt. 1, June 8, 1978, p. 24.

A legal opinion by an Executive Branch official cannot substitute for a court order under a legal scheme that says (with exceptions not relevant here) that court orders are the exclusive means of conducting surveillance. FISA's goal of establishing the exclusive legal foundation for national security electronic surveillance would be defeated if government officials and carriers could still rely on legal opinions or certifications issued outside the Act's exclusive framework.

It would wreak havoc on our laws if private sector parties could rely on Executive Branch opinions stating that something was legal when a statute had been enacted stating that the conduct was illegal except pursuant to conditions that were lacking in the particular instance. Such legal opinions issued outside of an exclusive legal framework are particularly unsuited in the context of national security, where the demands of secrecy and speed call for clarity of orders.

Questions Submitted by Senator Edward M. Kennedy

1. Mr. Dempsey, in your remarks at the hearing you said, "I've heard a lot of progress being made and I've heard the outlines of an approach that is better than the approach in the Protect America Act," and then you outlined several elements of that approach. I found your analysis very interesting and illuminating.

Question:

- **Can you please flesh out this approach? In particular, can you describe all the reforms that you think ought to be made to the Protect America Act, and indicate which ones you think would attract broad support and which ones would be controversial?**

Answer: In his oral answers to Senators' questions at the hearing, the DNI seemed to indicate that he agreed with certain core elements of a balanced statute: unambiguous language; court review and approval of the targeting and minimization rules; and particularized warrants for the intentional targeting of Americans regardless of geography. The difficulty, of course, is in implementing these elements in statutory language in a way that makes them meaningful. A particular barrier to the use of plain English is the Administration's unwillingness to state publicly the scope of what it is trying to authorize. Prior court review and approval of the targeting and minimization procedures, especially if it involves meaningful court supervision of the implementation of its orders, will be highly controversial, given the Administration's deep philosophical opposition to judicial checks and balances. The point about particularized orders for interceptions targeted at Americans abroad should not be controversial, primarily because such targeting of Americans abroad is rare.

To all Panel II Witnesses (James A. Baker, James X. Dempsey, Suzanne E. Spaulding, and Bryan Cunningham)

1. One thing the Administration rarely mentions in its statements about the Protect America Act is the Fourth Amendment. Yet the Constitution is the supreme law of the land, and all legislation must comply with it. There is obviously some uncertainty in Supreme Court case law about the extent to which the Fourth Amendment limits electronic surveillance, but we know from cases like *Katz* and *Keith* that the Fourth Amendment does apply in many situations.

Questions:

- **When Americans talk or e-mail with people overseas, does the Fourth Amendment provide any protection for their international communications?**

Answer: Americans communicating with persons abroad do retain some Fourth Amendment rights. This does not necessarily mean that a particularized warrant is required to target persons abroad while they are communicating with Americans.

However, a person who otherwise enjoys Fourth Amendment protection (in this case, an American inside the United States) does not loose all of those protections as soon as she communicates with a person who has no Fourth Amendment rights (in this case, a non-US person outside the United States). At the very least, the reasonableness clause of the Fourth Amendment still applies, and the Administration has never seriously argued that it does not. Indeed, the Administration has in effect admitted that the person in the US whose communications with someone abroad are intercepted has some rights, for the Administration has argued that a crucial component of even its approach is the minimization rules, which protect the rights of innocent Americans in the United States whose communications with foreigners are intercepted under a system targeting non-US persons abroad.

- **In your view, does the Protect America Act comply with the Fourth Amendment? If not, what are the offending provisions?**

Answer: Even if warrants are not needed for surveillance targeting persons overseas, the PAA falls far short of complying with the reasonableness clause of the Fourth Amendment because it does not set a sufficient standard for targeting in that it is not limited to searches of the communications of foreign powers or agents of foreign powers or those whose communications are for some other reason suspected of having intelligence value, it does not require minimization rules adequate to the specific problems associated with wholesale surveillance, it does not provide adequate judicial supervision of the conduct of the program, nor are searches reasonably limited in duration.

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."

- **What role should the FISA court have in safeguarding Americans' Fourth Amendment rights?**

Answer: The role of the FISA court should be threefold: (1) The court should review and approve in advance both the targeting procedures and the minimization procedures. (2) If the court finds that those procedures are reasonably designed to focus the surveillance and protect the rights of Americans, the court should issue an order authorizing the program of surveillance and ordering carriers upon whom the order is served to cooperate with the government in effectuating the surveillance, such that the surveillance is conducted pursuant to the order of the court, not pursuant to an assertion of Executive

Branch authority. (3) The court should conduct ongoing supervision of the implementation of its orders.

2. As you know, the Protect America Act weakens the role of the Foreign Intelligence Surveillance Court. For communications covered by the Act, the FISA court is permitted to conduct only a very general review of the government's collection procedures, long after the fact, under a "clearly erroneous" standard. That's a far cry from the central role that the Court has been playing under FISA.

The Administration has attempted to justify its undermining of the FISA court by claiming that more serious judicial review would be too burdensome, and that executive branch oversight is sufficient to make sure the law is not abused.

Questions:

- **How do you regard the Administration's arguments for why the FISA court should be marginalized?**
- **What role should judicial review have under any new legislation?**

Answers: The Administration's arguments have no support in logic or in practice. For thirty years, the FISA Court has proven that it is capable of responding quickly, in total secrecy, to surveillance requests. To the extent that there is a burden associated with the surveillance approval process, it is caused primarily by the layers of bureaucracy created within the Executive Branch.

Under any new legislation, the role of the court should be (1) review targeting and minimization procedures; (2) if it finds that the targeting procedures are reasonably designed to focus surveillance on the communications of non-US persons overseas reasonably believed to be involved in terrorist activity or otherwise reasonably believed likely to be of foreign intelligence value, and if it finds that the minimization procedures are reasonably likely to protect the rights of individuals against the dissemination of irrelevant or misleading information, issue an order authorizing a program of surveillance pursuant to such procedures; and (3) through periodic reports from the intelligence agencies, supervise the conduct of the surveillance and make such adjustments to its orders as are necessary to protect the rights of Americans.

3. Congressional oversight under the Protect America Act is also weak. Reports are made to Congress semi-annually. The only information that the Administration has to provide is the number of certifications and directives issued during the reporting period and descriptions of incidents of non-compliance.

Questions:

- **Are these reporting requirements adequate to ensure that Congress understands how the statute is affecting Americans and has the information necessary to fulfill its oversight responsibilities?**
- **What information does Congress need to conduct real oversight?**

Answers: These reporting requirements are woefully inadequate for several reasons. To begin with, under the PAA determinations of non-compliance by elements of the intelligence community rest solely with those entities themselves, meaning that the entities being overseen are able to determine what to disclose to the oversight committees. Moreover, the main focus of oversight should not be on matters that the Executive Branch determines to be non-compliance; to the contrary, given the breadth and ambiguity of the PAA, the focus of oversight should be on what the Administration concludes is compliance.

In order to conduct real oversight, Congress does not need information identifying individual targets. What Congress needs is information about how the Administration is interpreting and implementing FISA as amended by the PAA or other laws. This includes the targeting and minimization procedures, instructions to the intelligence agencies on how to interpret those procedures, legal memoranda interpreting FISA, briefs and other materials filed with the FISA court, and opinions issued by the court. Congress also needs information on the nature and volume of intercepted communications that involve a person in the US on one end of the communication and information about how those communications are handled.

4. The Administration is demanding that Congress grant retroactive immunity for communications service providers that complied with unlawful surveillance requests. Some of these companies apparently cooperated with the warrantless surveillance program, which violated FISA.

Questions:

- **How do you regard the Administration's argument that these companies must be granted full immunity or else they will go bankrupt? Aren't there other ways—such as a cap on damages—to prevent bankruptcy while still holding companies liable for violations of FISA?**
- **If bankruptcy is not the real issue, why is the Administration so adamant that retroactive immunity must be provided?**
- **Do you agree that provider liability is a key structural protection of FISA?**

Answers: There is indeed a range of options for protecting telecommunications companies from ruinous damages while still ensuring that FISA's exclusivity is enforced by sanctions on those who conduct surveillance contrary to the law. In our view, a cap on damages would be the most logical solution.

Since there are other solutions at hand, the Administration's adamant insistence on immunity seems to be part of its broader effort to undermine the rule of law. On a range of issues, the Administration has argued that it should be able to pick and choose what laws it follows. This approach seems guaranteed to weaken the national security, especially in the midst of what the Administration calls a war, when what is really needed is clarity and stability. Both intelligence officials and the companies on whose

cooperation the government relies need to be able to know what is legal or illegal. As we noted above, the purpose of FISA and its exclusivity clause was to make it crystal clear what was legal and what was illegal in the conduct of national security surveillance. For this reason alone, provider liability is a key structural protection of FISA: a system of national security law cannot function if the consequences for complying with the law (which grants immunity to companies that comply) are the same as the consequences for violating the law. That is a recipe for confusion and hesitation.

5. Many of us are obviously concerned about the scope of the Protect America Act. The Act isn't clear in many respects, but it seems to authorize very broad warrantless surveillance—far broader than anything allowed under FISA.

Questions:

- **Under the Protect America Act, would it be lawful to collect every communication from America to Germany—without a court warrant—if the purpose of this collection was to find one terrorist in Germany?**
    - **How could the Act be amended to place some constraints on such activity?**

Answers: The PAA was fatally ambiguous, and the Administration never clearly described on the public record how it would interpret the Act. However, one reading of the PAA is that it would have permitted the collection of every communication between America and Germany. To avoid such an interpretation and place reasonable constraints on the government's surveillance activity, the Act could have been amended to authorize surveillance only when the intelligence agencies were targeting a particular person or phone line or email account and there was reason to believe that intelligence information would be obtained from the communications of the targeted person.

- **Does the Protect America Act cover stored communications—for instance, e-mails sitting in a person's mailbox—as well as real-time communications?**

Answer: Yes.

    - **Is this a significant change in the law? Why does it matter?**

Answer: It is may understanding that, even before the PAA, FISA had been interpreted as authorizing access to stored email, although I do not fully understand what theory the government proceeded under. (The rationale may itself be classified, illustrating one of the longstanding problems with the application of FISA.) The standards for access to stored email matter because individuals are storing more and more email with service providers, covering many years of personal and professional activity, greatly augmenting the reach of the government's surveillance. The government should be able to access this information, but only under strict standards.

- **Why did the Administration insist on the phrase "concerning," rather than "directed at," when describing surveillance in Section 105B? Isn't "concerning" a significantly broader term?**

Answer: The DNI testified at the September 25 hearing that he did not remember why the word "concerning" was used, but it certainly seems to have been intended to give the Administration broad latitude in applying the Act.

- **In general, would you say that the Protect America Act simply "modernizes" FISA to account for changes in technology and security threats? Or does the Act overturn FISA in key respects?**

Answer: The PAA was in no way a modernization effort; instead, as you suggest, it was intended to carve a huge loophole in the Act, while deferring true modernization. Among many indications that the PAA is not a serious effort at modernization: it does not seek to clarify FISA's definition of "content," and does not even address the difference between content and transactional data, a key distinction in both the technology and under the Constitution; the implementation of the PAA hinges on the government's being able to determine the geographic location of the person who is being targeted, even though intelligence officials have testified that one of the key technological changes they face is that it is increasingly difficult to tell where a person is located; it makes no changes to the definition of "minimization," which was intended to apply to particularized surveillance pursuant to a court order, not to the generalized, warrantless surveillance the PAA authorizes.

6. The Administration has repeatedly claimed that the Protect America Act restores FISA's original intent. One aspect of this claim is that FISA was never intended to protect Americans who communicate with foreign targets. Director of National Intelligence McConnell has stated that "Congress crafted [FISA] specifically to exclude the Intelligence Community's surveillance operations against targets outside the United States, including where those targets were in communication with Americans, so long as the U.S. side of that communication was not the real target."

Questions:

- **Is this claim by the Administration correct?**
- **Even if the Administration's claim is correct, do you think it's appropriate to provide as little protection as this statute provides for Americans whose communications may be "incidentally" collected by the government?**

Answers: The Administration's claim is not correct. Contrary to the DNI's statement, the original FISA did apply to the Intelligence Community's surveillance operations against targets outside of the United States, where the communications of those targets were intercepted off a wire inside the US. Only radio communications were exempt from the original FISA. The intent of that exception is now lost; neither the Administration nor the opponents of the PAA have been able to conclusively explain the intent of the

radio exception. The exception may have been intended mainly to exclude foreign-to-foreign radio communications, which might have been accessible from inside the US. In any event, as noted above, the original intent of FISA with respect to foreign-to-domestic communications has limited relevance today, after dramatic changes in the business and family relationships of ordinary Americans have left many citizens heavily dependent on international communications in their daily lives. In today's environment, a collection program targeting persons abroad is far more likely to pick up communications with citizens inside the US, requiring greater protections than afforded by the PAA.

7. Under the Protect America Act, it is possible that millions of "incidental" communications between foreign targets and innocent American citizens will be collected by the government. Many of us are concerned that the Intelligence Community's minimization procedures—the procedures that control what can be done with information after it has been collected—are insufficient to protect the privacy of these Americans.

Questions:

- **To the best of your knowledge, what limits currently exist on the government's ability to store, analyze, and disseminate information it collects without a FISA warrant on Americans who were never a target?**
- **Should new legislation require stronger minimization procedures, either for all Americans' communications or at least for international communications that are "incidentally" collected?**

Answers: CDT has extensively analyzed the current minimization procedures and explained why they are inadequate to protect the rights of Americans, in a memo published at http://www.cdt.org/security/20070917mimization-memo.pdf. In sum, the procedures give the government broad discretion to store, analyze and disseminate information collected with or without a warrant about Americans who were never a target. New legislation should require stronger minimization procedures.

8. It appears from the text of the Protect America Act that Americans who travel abroad are now extremely vulnerable to warrantless surveillance. When Americans travel out of the country, the Act suggests that the government can wiretap them—without any warrant—as long as a significant purpose of the surveillance is to obtain foreign intelligence information.

Questions:

- **Is this correct?**

Answer: FISA as originally enacted did not apply to any surveillance conducted outside the US, whether or not it was targeted against Americans. As originally enacted, FISA applied to the communications of Americans abroad only to the extent that those communications were with someone in the US and the communication was intercepted from a wire inside the US. That is, the original FISA did not give any special protection

to Americans abroad: Americans abroad received the same treatment as other persons abroad, in that a court order was required to intercept in the US wire communications with one party in the US and one party abroad; it made no difference whether the party abroad was a US person or a non-US person. The change wrought by the PAA affects Americans abroad to the extent that it allows more interception of calls between people in the US and people abroad of any nationality, but the far bigger effect of the Act is on Americans in the US, since their communications with people abroad are all subject to warrantless and essentially standardless surveillance.

- **Can you explain what effect Executive Order 12333 has on the wiretapping of Americans abroad, and whether this Order will continue to have force under the Protect America Act?**

Answer: For the targeted wiretapping of Americans abroad, EO 12333 requires that the Attorney General determine in each case that there is probable cause to believe that the American is a foreign power or an agent of a foreign power. It does not appear that the PAA had any impact on that administrative rule.

- **To protect the rights of Americans who travel abroad, should we require a warrant anytime the government wants to target a U.S. citizen?**

Answer: Yes.

9. We spent much of the hearing debating the Protect America Act, which is very controversial and troubling in itself. But the Administration is also asking for additional changes in the FISA law. For example, Director McConnell has asked for a variety of "streamlining" measures and for an extension of FISA's emergency provision from 72 hours to one week.

Questions:

- **What do you think of these new requests?**

Answer: It seems unnecessary to extend the 72 hour emergency rule.

- **Beyond this debate we are having over FISA and the Protect America Act, what else does Congress need to do to ensure that our intelligence programs are as effective and responsible as possible?**
    - **It has been reported that the National Security Agency is having many problems with management and with the computational and translational aspects of intelligence analysis. Should these be priorities?**

Answers: Congress needs to take a comprehensive look at the collection, analysis and information sharing activities of the intelligence agencies. This review would be especially beneficial if it looked at both the effectiveness and the civil liberties

implications of such activities, for there are grounds for concern that the intelligence agencies are less than effective at analyzing the information they already collect while, at the same time, the Administration is seeking authority to acquire even more data. Such an inquiry should examine not only real-time surveillance but also access to stored data, including stored transactional data regarding communications services, travel, and financial activity. Also, attention needs to be paid to how this information is being interpreted and used. For example, there is no doubt that the terrorist watch list is plagued by inaccurate and misleading information, a situation that is equally dangerous to national security and to civil liberties.

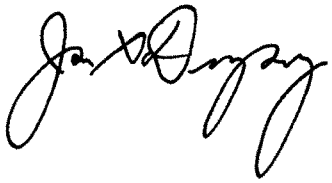
- **Unfortunately, a majority of this Committee is hampered in this debate by not knowing precisely what we are fixing. Despite subpoenas, we have been denied the legal justifications for the warrantless surveillance program, and we have been denied access to the FISA court opinions that we are told made new legislation necessary. We are being told we need to fix a problem whose nature and scope have not been revealed to us.**
    - **Given the secrecy that enshrouds this entire debate, how would you recommend Congress fulfill its oversight responsibility?**
    - **Do you think Congress should conduct a broader review of intelligence policy at this time?**

Answers: The Congress has available to it a number of tools to secure the information it needs to carry out its responsibilities. It can, for example, decline to confirm Administration appointees until certain information is forthcoming. It can use the power of the purse to withhold or condition funds. It can, of course, seek enforcement of its subpoenas. Senators can place holds on legislation, related or unrelated to the information being sought. All of these levers have their limits, especially since the activities at issue are crucial to the national security. The best results for the country will emerge from the steady, consistent application of all these mechanisms.

* * *

As always, the Center for Democracy & Technology is honored to be asked to present its views to the Committee. We look forward to working with all members of the Committee to achieve true, balanced FISA reform.

Sincerely,



James X. Dempsey
Vice President for Public Policy

"Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?" September 25, 2007

Questions for the Record Submitted by Ranking Member Arlen Specter

Questions for Director of National Intelligence J. Michael McConnell

1. **How targeted is the surveillance being conducted pursuant to the Protect America Act?** In your August 22, 2007 interview with the *El Paso Times*, you said: "Now there's a sense that we're doing massive data mining. In fact, what we're doing is surgical. A telephone number is surgical. So, if you know what number, you can select it out." To the extent you can comment in an unclassified format, can you elaborate on how targeted the surveillance being pursued under the Protect America Act is?

2. **Do you interpret the Protect America Act to authorize a range of intelligence gathering activities?** In a July 31, 2007 letter to me, you indicated that the activity that has come to be known as the "Terrorist Surveillance Program" was just one "aspect" of the "various intelligence activities" authorized by the President after 9/11. Do you believe the Protect America Act encompasses or authorizes intelligence activities beyond the acquisition of communications that would constitute "electronic surveillance" under Section 101(f) of the Foreign Intelligence Surveillance Act (FISA), *but for* the exception to that definition created by new Section 105A of FISA?

3. **Protections for U.S. persons located overseas.** The Protect America Act refers to surveillance "directed at *a person* reasonably believed to be located outside of the United States," rather than limiting the scope of surveillance to *foreign persons*. Nevertheless, you have pointed out that Executive Order 12333, Section 2.5, already prohibits surveillance of U.S. persons overseas unless the Attorney General determines "in each case that there is probable cause to believe" the person is "a foreign power or an agent of a foreign power."

   At the hearing, you said you "would have no personal objection" to transferring the authority to approve surveillance of U.S. persons overseas to the Foreign Intelligence Surveillance Court, and codifying the required probable cause showing. Nevertheless, you cautioned against potential unintended consequences of such a change, and you highlighted the possible need to differentiate between U.S. persons and U.S. citizens.

   a. Having considered the issue, have you identified any potential concerns with such a change in the law? Does your analysis depend upon whether the collection of intelligence occurs inside the United States or outside the United States?

53358.056

b. Can you elaborate on the implications of providing such protections to all U.S. persons, as compared to just U.S. citizens? Does the Executive Order recognize this distinction for purpose of Section 2.5?

4. **Use of the terms "concerning" and "directed at" in the Protect America Act.** In response to question from Sen. Feingold, you acknowledged some possible ambivalence about the choice of the terms "concerning" and "directed at" in different parts of the Protect America Act. Have you determined whether the terms "directed at" or "targeted at" could be used throughout the legislation without negative consequences for the collection of foreign intelligence?

Question for Bryan Cunningham

At the hearing, I asked you about the possibility of requiring the government to report back to the Foreign Intelligence Surveillance Court periodically about the surveillance conducted pursuant to the Protect America Act. You expressed concerns about having the court "evaluate the foreign intelligence value of the information" collected. Nevertheless, you suggested that it may be appropriate to have the court evaluate whether "the scope of the intercepts really worked" as contemplated. Could you elaborate on the type of review you would consider appropriate when the court is asked to reauthorize the government's surveillance procedures, including the appropriate standard of review?

Questions for Suzanne Spaulding

1. At the hearing, you testified that Congress should avoid creating exceptions to FISA's definition of "electronic surveillance," to prevent negating statutory protections linked to that definition. Nevertheless, given that the existing definition of electronic surveillance still distinguishes between "wire" and "radio" communications, would you support amending the definition to make it technology neutral?

2. In your testimony, you state that legislation reauthorizing or modifying the Protect America Act should limit the statute's scope to the collection of intelligence concerning terrorism, rather than the collection of foreign intelligence more broadly. DNI McConnell has testified, however, that our nation faces other equally pressing concerns, such as foreign intelligence involving the proliferation of weapons of mass destruction.

    a. Do you continue to believe that new legislation should not encompass foreign intelligence related to the proliferation of weapons of mass destruction and similar threats to our national security?

53358.057

b. Are you worried that distinguishing between different categories of foreign intelligence might unnecessarily complicate the guidance and training provided to intelligence officers?

Question for James X. Dempsey

Your written testimony states: "a communications service provider should not have to guess whether cooperation with an apparently illegal request will be excused." Would your analysis of the arguments for retroactive immunity change if the requests received by communications carriers were not "apparently illegal"? Would it be different, for example, if the carriers received a certification of the program's legality?

Questions for James A. Baker

1. In Jack Goldsmith's recent book, *The Terror Presidency: Law and Judgment Inside the Bush Administration*, Mr. Goldsmith writes: "Jim Baker analogizes the task of stopping our enemy to a goalie in a soccer game who 'must stop every shot, for the enemy wins if it scores a single goal.' The problem, Baker says, 'is that the goalie cannot see the ball—it is invisible. So are the players—he doesn't know how many there are, or where they are, or what they look like. He doesn't know where the sidelines are—they are blurry and constantly shifting, as are the rules of the game itself.'" (Emphasis added.)
   c. Is Mr. Goldsmith right to credit you, among others, with the soccer goalie analogy?
   d. What does the goalie analogy portend for our decisions about whether to renew the Protect America Act? Specifically, what are we to do when NSA analysts and DNI McConnell tell us that they cannot know in advance whether a terrorist overseas will call into the US?

2. Given your knowledge of the Foreign Intelligence Surveillance Court, how do you believe that court would react to an expansion of its jurisdiction to include approval of surveillance targeting U.S. persons overseas – if, for example, the authority granted to the Attorney General under Section 2.5 of Executive Order 12333 was transferred to the court by statute?

53358.058

Questions of Senator Dick Durbin
Senate Judiciary Committee Hearing
"Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?"
September 25, 2007

Director of National Intelligence J. Michael McConnell

1. The Administration has taken the position that the President is not required to follow certain laws that he believes interfere with his power as Commander in Chief. Apparently that is the Administration's view of the Protect America Act. According to *The New York Times*:

   > [S]enior Justice Department officials refused to commit the administration to adhering to the limits laid out in the new legislation and left open the possibility that the president could once again use what they have said in other instances is his constitutional authority to act outside the regulations set by Congress.

   Will you pledge that the Intelligence Community will comply with the Protect America Act in all circumstances?

2. I received a letter from a constituent expressing concern that he might be subject to NSA surveillance because he corresponds by e-mail with a journalist in Iraq who writes for *The Chicago Tribune*. He wrote to the NSA to ask whether his communications have been subject to NSA surveillance. He received a response from the NSA that said the NSA "can neither confirm nor deny" that he has been subject to warrantless surveillance.

   a. Under the Protect America Act, could my constituent be subject to warrantless surveillance?
   b. Could American servicemembers overseas who call and e-mail their families in the U.S. be subject to warrantless surveillance under the Protect America Act?
   c. What assurances can you provide to innocent Americans that the NSA is not listening to their phone calls and reading their e-mails?

3. Some experts have concluded that the Protect America Act is so broadly drafted that it authorizes the government to gather the sensitive personal records of innocent American citizens in this country as long as you and the Attorney General certify the information "concern[s] persons reasonably believed to be outside the United States." Do you agree with this interpretation?

4. If the government does not intend to use the Protect America Act to seize the records of innocent Americans in the U.S., would you support revising the law to make this clear?

5. Some have proposed that the Protect America Act be revised as follows: the government would not be required to obtain a warrant for any surveillance where the target is reasonably believed to be outside the U.S., but the government would later be required to apply for a warrant if there is reason to believe that a "significant number" of intercepted communications involve a person who is in the U.S. Would you support revising the law in this way?

53358.059

6. Some experts have proposed that the FISA court should review the government's surveillance procedures to ensure that they are reasonably likely to target non-U.S. persons outside the U.S. and collect foreign intelligence information. Would you support revising the law in this way?

53358.060

Senate Judiciary Committee
Hearing on "Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?"
Tuesday, September 25, 2007

Questions Submitted by U.S. Senator Russell D. Feingold to Director of National Intelligence J. Michael McConnell

1. In your opinion, should the Judiciary and Intelligence Committees be provided access to the Presidential Authorizations and Office of Legal Counsel opinions justifying the NSA warrantless wiretapping program, from 2001 to the present?

2. During the hearing, you testified that you could provide the Judiciary Committee, in a matter of weeks, with information about how much U.S. person information is looked at and disseminated under the new Protect America Act authorities. Please provide that information as soon as it becomes available.

3. The Protect America Act contains a provision that permits communications providers directed to conduct surveillance under that law to file a petition with the FISA Court challenging the legality of the directive.

    a. Will you commit to notifying the Judiciary and Intelligence Committees if any such petitions are filed with the FISA Court challenging the Protect America Act, and will you share with those committees any court action, as well as the pleadings in those proceedings, redacted as necessary?
    b. Will you commit to announcing, publicly, the fact that such a petition has been filed?

4. The Protect America Act authorizes surveillance directed at individuals 'reasonably' believed to be overseas, subject only to after-the-fact, "clear error" review by the FISA Court of the procedures for making that determination. If an American inside the United States were accidentally targeted under Protect America Act authorities, or if purely domestic communications were accidentally acquired, what happens to those communications?

5. The Protect America Act provides that FISA warrants are not required for surveillance "directed at" a person outside the United States. FISA uses the term "targeting," and according to the testimony of James Baker, intelligence professionals clearly understand what is meant by the term "targeting."

    a. What, if anything, is the difference between "directing" surveillance at a person, and "targeting" that person for surveillance?

53358.061

b. If there is no difference, for the sake of clarity why not use the word "targeting"?

6. You have argued that the Protect America Act simply implements the intent of Congress in 1978, because FISA was originally intended to permit the Intelligence Community to intercept all communications of Americans with foreign countries without a court order, as long as individuals in the U.S. were not targets. Your support for this is that FISA permitted the interception of all international radio communications, and that, according to your testimony, "almost all" communications between the U.S. and other countries in 1978 were considered radio.

   Two of the witnesses who testified on the second panel presented a different factual picture of the state of technology in the late 1970s. In their written testimony, Jim Baker, the former head of the Office of Intelligence and Policy Review at DOJ, and Jim Dempsey of the Center for Democracy & Technology, explain that international communications occurred both by satellite and undersea cable in the 1970s. In addition, FISA itself specifically required a warrant for some communications between the U.S. and overseas. Would you like to reconsider your assertion that FISA was originally intended to permit the government to intercept all international communications of individuals in the United States, without a warrant?

7. On its face, Section 105B of the Protect America Act is not mandatory. It is optional, meaning that the Intelligence Community could conduct surveillance of any individual overseas without fulfilling even the procedures in Section 105B. Do you agree that it is not a statutory requirement that the government follow the procedures laid out in Section 105B?

8. Does the President have authority to authorize electronic surveillance beyond what is permitted by FISA as amended by the Protect America Act?

9. Under the Protect America Act, what role is assigned to the FISA Court to play in developing and ensuring compliance with minimization procedures?

10. Is there a greater potential for intrusions on Americans' privacy rights, mistaken or otherwise, if the government is intercepting international communications in the United States, as opposed to when the interception occurs overseas?

11. Senator Leahy asked you about the minimization rules under the Protect America Act, and you told him that "if you're minimizing, you would take them out of the database." What are you referring to? Please clarify this statement.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00129 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.062

Senator Edward M. Kennedy
Questions for the Record
From Senate Judiciary Committee hearing on "Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?"
Held on September 25, 2007

To Director of National Intelligence Mike McConnell

1. As the history of U.S. surveillance law teaches us, it is essential that we have a very careful and—to the fullest extent possible—public consideration of FISA legislation.

I was present at the creation of the FISA law, and I worked closely with a Republican Attorney General to draft its provisions. Together, we found a way to provide our intelligence agencies with the tools they needed, while building in checks and balances to prevent abuse of those tools. FISA proved that often we do not have to choose between civil liberties and national security.

Unfortunately, the Protect America Act was enacted in a much less thoughtful process. It was negotiated in secret and at the last minute, while the Administration issued dire threats that failure to enact a bill before the August recess this summer could lead to disaster. We need to correct that failure by engaging in a thorough, deliberative process before we enact more legislation.

That process cannot begin if the Administration asks us to legislate in the dark. The Administration has failed to provide us with adequate information about its activities, the legal justifications for those activities, and the FISA court opinions that we are told make new legislation necessary. I hope this hearing will mark the beginning of the end of this stonewalling.

Questions:

- **Will you provide us with the information we need to make informed judgments about whether FISA needs to be reformed?**
- **Will you provide us with the legal justifications pursuant to which the Administration conducted warrantless surveillance of Americans?**
- **Will you provide us with details regarding the manner in which that surveillance was conducted?**

2. I was upset to read your comment in the *El Paso Times* that because we are debating FISA reform in Congress, "Americans are going to die." As you know, Congress takes great pains to protect classified secrets, and we are absolutely committed to protecting our country. Terrorists are well aware that their communications may be monitored.

Question:

- **Do you continue to maintain that "Americans are going to die" because of this debate?**

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00130 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.063

3. In the same *El Paso Times* interview, you discussed the two opinions by the FISA court that you say made new legislation necessary. You revealed that the first judge ruled that "what we needed to do we could do with an approval process that was at the summary level." You said, "the second judge looked at the same data and said well wait a minute I interpret the law, which is the FISA law, differently. And it came down to, if it's on a wire and it's foreign in a foreign country, you have to have a warrant . . . ."

In making these statements, you told the *El Paso Times* about FISA court opinions that the Administration has refused to share with Congress.

Questions:

- **Can you explain why you chose to leak these details?**
- **Do you stand by all the statements you made to the *El Paso Times*? For instance, do you stand by the statements that only about 100 people inside the U.S. are currently under surveillance by intelligence agencies and that "[i]t takes about 200 man hours to do one telephone number" for the FISA court?**
- **Will you make the two FISA court decisions you discussed available to the Committee?**

4. The Administration has asserted a view of executive power that is breathtaking in scope. It has claimed the authority to wiretap Americans without warrants, despite the clear statement in FISA that it provides the "exclusive" means for conducting foreign intelligence surveillance. As we know from Justice Jackson's opinion in the Steel Seizure Cases, the President's authority is at its weakest when he acts contrary to a congressional enactment. Yet President Bush defied clear statutory language.

It is disturbing that officials in the Administration find it so difficult to state that they will obey the law. The right and ability of Congress to be a check on the executive branch is a bedrock principle of our constitutional system. Yet the Administration is asking for our consent to a new law, while simultaneously insisting that no such consent is necessary.

Questions:

- **If we enact a new FISA bill, will the President and the Intelligence Community accept that they are bound by it? In particular, if we pass a bill that gives the President and the Intelligence Community less power to conduct surveillance than they are now exercising, will they comply with it?**
- **If we do not extend the Protect America Act and do not pass any other new laws, will the Administration comply with FISA?**
- **Are any electronic surveillance programs currently being conducted outside the authority of FISA as amended by the Protect America Act?**
- **Do you agree that new legislation should reaffirm that FISA is the sole means by which the executive branch can intercept communications in the United States?**

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00131 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.064

5. The Administration is asking Congress to grant broad immunity for any past violations of the law by communications companies that provided surveillance information.

Once again, the enactment of FISA shows us the right way to handle this issue. Under that carefully drafted statute, communications carriers have immunity from liability if they act pursuant to a court warrant or a certification from the Attorney General that the matter falls within one of the statutory exceptions that permits surveillance without a warrant. In this way, FISA protects carriers who follow the law.

Unfortunately, the Administration is now seeking immunity for carriers that violated FISA. Worse, the Administration will not tell us which carriers participated in the warrantless surveillance program, the nature or scope of their law-breaking, or why they deserve immunity for their actions. Once again, the Administration is asking Congress to legislate in the dark.

I'm troubled that the Administration apparently encouraged communications companies to break the law, and that those companies apparently went along. Our democracy cannot tolerate an executive branch that picks and chooses which laws to obey, and then asks others to do the same. How can we in Congress, as responsible lawmakers, vote to immunize any persons or companies until we have a full explanation of what they did and why they did it?

Questions:

- **Isn't it true that carriers who acted pursuant to a warrant or the Attorney General's certification already have immunity from liability? If the warrantless surveillance program was legal as you have claimed, what do carriers need immunity from?**
- **Wouldn't Congress be endorsing the warrantless spying program by granting broad immunity?**
- **If Congress immunizes any companies that may have broken the law, won't that set a bad precedent? What incentive will companies have in the future to follow the law and protect Americans' sensitive information?**
- **If your concern is that carriers not be bankrupted, would you support something more specific than complete amnesty—for example, a cap on damages?**
    - **If not, why not? Are you worried that courts will rule that the President's warrantless surveillance programs were illegal?**

6. The Protect America Act contains remarkably broad language. Under one provision, the Administration does not need a FISA warrant to intercept any communications "concerning persons reasonably believed to be outside the United States," so long as a significant purpose of the surveillance is to obtain foreign intelligence information—a term that sweeps much broader than terrorism—and reasonable procedures are in place.

As you know, there has been a great deal of confusion about what this provision authorizes, and many Americans are concerned that it goes too far. Along with Assistant Attorney General for National Security Kenneth Wainstein, you have tried to allay some of these concerns in public statements.

Specifically, both of you have said that, when properly read, the Protect America Act does *not* authorize:

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00132 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.065

1. warrantless surveillance of domestic-to-domestic communications (on the theory that these communications might "concern" a foreign target);
2. warrantless physical searches of the homes, mail, computers, or effects of individuals in the United States;
3. warrantless acquisition of the business records (including library and medical records) of individuals in the United States; or
4. "reverse targeting" of U.S. persons, in which the government does warrantless surveillance of a person overseas when its primary or coequal purpose is to surveil a person inside the United States with whom the overseas person is communicating.

These activities, you have said, are *not* lawful under the Act. My concern is that it is not sufficiently clear from the statute that these activities are prohibited.

Questions:

- **Since the Protect America Act is not clear about whether or not it prohibits such troubling practices, will you work with Congress on statutory language that clearly prohibits them?**
    - **If you will not make this commitment, why not? This is a statute that will remain in place after you have left office. Unless the statute is clear, how can we trust that the government will not try to read ambiguous provisions as broadly as it can?**

7. Several other features of the Protect America Act are troubling. There is little debate about what these features do. Their language is clear. It is the substance of these features that concerns me, because in my view they do not comply with the original intent of FISA.

Judicial review under the Protect America Act is extremely weak. The FISA court only gets to look at the procedures for ensuring that persons being targeted are outside the U.S. and that acquisitions conducted under Section 105B do not constitute electronic surveillance. This review occurs long after the fact, under a "clearly erroneous" standard.

This is far from the independent judicial review that FISA has always used to protect Americans. Some people resisted judicial oversight then just as they are resisting it now, but it has worked to safeguard Americans' security as well as their liberty, by ensuring that government surveillance activities are legal. The FISA court has been overseeing spying activities that touch American soil for nearly 30 years, without incident.

Also, congressional oversight under the Protect America Act is very weak. Reports are made to Congress semi-annually. The only information the Administration must provide is certain aggregate data (the number of certifications and directives issued during the reporting period) and descriptions of incidents of non-compliance. There is nothing in the statute to guarantee that Congress will learn how the statute is affecting Americans.

Further, there is no mechanism in the Act to ensure adequate protection for Americans' communications that are "incidentally" collected when the government is targeting someone overseas. For example, there is no requirement that these communications be minimized in any particular way. To the contrary, it seems that under the Act, the government can use and disseminate these communications as it wishes. There is no requirement that if a particular

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00133 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.066

American is "incidentally" wiretapped at great length, the government will at any point need to obtain a warrant.

Questions:

- **Would you accept a stronger role for judicial review under new legislation?**
  - **For example, would you accept a role for the FISA court in reviewing the Intelligence Community's targeting and filtering procedures *before* these procedures go into effect?**
  - **Would you accept a standard of review higher than "clearly erroneous"?**
  - **There have been many complaints from the Administration that the FISA process is too burdensome. If this is one reason you want to minimize judicial oversight, can you explain why it would not meet your needs to have additional resources or more time to seek after-the-fact emergency warrants?**
- **Would you accept a stronger role for congressional review under new legislation?**
  - **For example, would you accept a requirement that the Administration report to Congress (in a classified setting, if necessary) how many Americans' communications were surveilled in the reporting period?**
- **Would you accept new rules that provide more protection for Americans whose communications are "incidentally" collected?**
  - **For example, would you accept special, enhanced minimization procedures for such collections?**
  - **Would you accept a requirement that if any particular American is "incidentally" surveilled in a sustained way, at some point a court warrant will be required?**

8. One of the unfortunate consequences of the way the Protect America Act was passed is that there is still great confusion—even among members of Congress—about what it does and does not authorize. The statute itself is ambiguous in many places, and there is hardly any record in Congress to help interpret it. As Mort Halperin said to the House Committee on the Judiciary, "Congress enacted legislation the meaning of which is simply not deducible from the words in the text."

If the Administration had been more willing to work with Congress, we would have had an opportunity to ensure that the new legislation was clear, complied with the Constitution, and struck the proper balance between security and liberty. Instead, as Mr. Halperin said, "[t]he bipartisan and strong public support of the FISA was ruptured by the Administration's tactics."

I am not asking you at this time to go over every ambiguity in the statute, but I have questions about several provisions that are particularly unclear. It is important to learn what these provisions do and do not authorize in order to evaluate them effectively.

Questions:

- **Section 105A of the Protect America Act refers to activities "directed at" persons abroad, while Section 105B refers to activities "concerning" such persons. Previous**

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00134 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.067

drafts of the statute had used "directed at" in both sections. However, "concerning" appears to be a much broader term.
  - **Why did the Administration insist on changing the language in Section 105B to "concerning"?**
  - **How do you plan on interpreting the "concerning" language?**
- **I am concerned about the phrase "other persons" in Section 105B(a)(3) of the Act. Who are these other persons that the Administration can now order to turn over communications? The Postal Service? Federal Express? Private individuals?**
- **I am also concerned about the potential breadth of Section 105B. Under the Protect America Act, would it be lawful to collect every communication from America to Germany—without a court warrant—if the purpose of this collection was to find one terrorist in Germany?**
  - **If not, please explain why this would be unlawful under the statute.**
  - **If this would be lawful, don't you find it troubling that potentially millions of communications could be intercepted in this way—without any court warrant—to find a single foreign target?**
  - **Will you work with Congress to find language that will place limits on overbroad warrantless surveillance?**
- **Does the Protect America Act cover stored communications—for instance, e-mails sitting in a person's mailbox—as well as real-time communications?**
  - **If not, where in the statute does it indicate that stored communications may not be collected under the Act?**
  - **If so, isn't this a significant change from the traditional FISA regime of intercepting real-time communications only?**
- **Under the Protect America Act, certifications are "not required to identify the specific facilities, places, premises, or property" that the government will be able to access.**
  - **Why not?**
  - **Does this mean that once it has a certification, the government will be able to collect any information it wants from a communications provider?**

9. The Protect America Act gives the Administration great power to conduct warrantless surveillance of "persons reasonably believed to be outside the United States." Some of these persons might be U.S. citizens traveling or living abroad.

An Executive Order (12333) provides some limits on surveillance of U.S. citizens who are abroad. But it is just an Executive Order, and we all know that statutes can trump Executive Orders. Along with colleagues like Senator Whitehouse who have raised this issue, I am worried that under the Protect America Act, the Administration will be able to wiretap at will soldiers serving in Iraq, or Americans visiting relatives in other countries, or Americans studying or doing business abroad. Most Americans would be upset to learn that the government can do this.

Questions:

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00135 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.088

- **If you agree that Americans who travel abroad do not sacrifice all their civil liberties and privacy rights at the border, will you work with Congress to make sure that new legislation recognizes privacy protections for Americans abroad?**
- **Do you believe that before the government can target a U.S. person abroad, a court warrant should be required?**
    - **If not, why should FISA's most central protection of Americans—that a warrant be required before their communications can intentionally be surveilled—suddenly disappear the moment they step over the border?**
- **If you are unwilling to require a FISA court warrant for surveillance that targets Americans abroad, would you be willing to codify in statute the standards and procedures of Executive Order 12333 for this surveillance?**

To James X. Dempsey

1. Mr. Dempsey, in your remarks at the hearing you said, "I've heard a lot of progress being made and I've heard the outlines of an approach that is better than the approach in the Protect America Act," and then you outlined several elements of that approach. I found your analysis very interesting and illuminating.

Question:

- **Can you please flesh out this approach? In particular, can you describe all the reforms that you think ought to be made to the Protect America Act, and indicate which ones you think would attract broad support and which ones would be controversial?**

To all Panel II Witnesses (James A. Baker, James X. Dempsey, Suzanne E. Spaulding, and Bryan Cunningham)

1. One thing the Administration rarely mentions in its statements about the Protect America Act is the Fourth Amendment. Yet the Constitution is the supreme law of the land, and all legislation must comply with it. There is obviously some uncertainty in Supreme Court case law about the extent to which the Fourth Amendment limits electronic surveillance, but we know from cases like *Katz* and *Keith* that the Fourth Amendment does apply in many situations.

Questions:

- **When Americans talk or e-mail with people overseas, does the Fourth Amendment provide any protection for their international communications?**

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00136 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.069

- **In your view, does the Protect America Act comply with the Fourth Amendment? If not, what are the offending provisions?**
- **What role should the FISA court have in safeguarding Americans' Fourth Amendment rights?**

2. As you know, the Protect America Act weakens the role of the Foreign Intelligence Surveillance Court. For communications covered by the Act, the FISA court is permitted to conduct only a very general review of the government's collection procedures, long after the fact, under a "clearly erroneous" standard. That's a far cry from the central role that the Court has been playing under FISA.

The Administration has attempted to justify its undermining of the FISA court by claiming that more serious judicial review would be too burdensome, and that executive branch oversight is sufficient to make sure the law is not abused.

Questions:

- **How do you regard the Administration's arguments for why the FISA court should be marginalized?**
- **What role should judicial review have under any new legislation?**

3. Congressional oversight under the Protect America Act is also weak. Reports are made to Congress semi-annually. The only information that the Administration has to provide is the number of certifications and directives issued during the reporting period and descriptions of incidents of non-compliance.

Questions:

- **Are these reporting requirements adequate to ensure that Congress understands how the statute is affecting Americans and has the information necessary to fulfill its oversight responsibilities?**
- **What information does Congress need to conduct real oversight?**

4. The Administration is demanding that Congress grant retroactive immunity for communications service providers that complied with unlawful surveillance requests. Some of these companies apparently cooperated with the warrantless surveillance program, which violated FISA.

Questions:

- **How do you regard the Administration's argument that these companies must be granted full immunity or else they will go bankrupt? Aren't there other ways—such as a cap on damages—to prevent bankruptcy while still holding companies liable for violations of FISA?**

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00137 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.070

- **If bankruptcy is not the real issue, why is the Administration so adamant that retroactive immunity must be provided?**
- **Do you agree that provider liability is a key structural protection of FISA?**

5. Many of us are obviously concerned about the scope of the Protect America Act. The Act isn't clear in many respects, but it seems to authorize very broad warrantless surveillance—far broader than anything allowed under FISA.

Questions:

- **Under the Protect America Act, would it be lawful to collect every communication from America to Germany—without a court warrant—if the purpose of this collection was to find one terrorist in Germany?**
    - **How could the Act be amended to place some constraints on such activity?**
- **Does the Protect America Act cover stored communications—for instance, e-mails sitting in a person's mailbox—as well as real-time communications?**
    - **Is this a significant change in the law? Why does it matter?**
- **Why did the Administration insist on the phrase "concerning," rather than "directed at," when describing surveillance in Section 105B? Isn't "concerning" a significantly broader term?**
- **In general, would you say that the Protect America Act simply "modernizes" FISA to account for changes in technology and security threats? Or does the Act overturn FISA in key respects?**

6. The Administration has repeatedly claimed that the Protect America Act restores FISA's original intent. One aspect of this claim is that FISA was never intended to protect Americans who communicate with foreign targets. Director of National Intelligence McConnell has stated that "Congress crafted [FISA] specifically to exclude the Intelligence Community's surveillance operations against targets outside the United States, including where those targets were in communication with Americans, so long as the U.S. side of that communication was not the real target."

Questions:

- **Is this claim by the Administration correct?**
- **Even if the Administration's claim is correct, do you think it's appropriate to provide as little protection as this statute provides for Americans whose communications may be "incidentally" collected by the government?**

7. Under the Protect America Act, it is possible that millions of "incidental" communications between foreign targets and innocent American citizens will be collected by the government. Many of us are concerned that the Intelligence Community's minimization

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00138 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.071

procedures—the procedures that control what can be done with information after it has been collected—are insufficient to protect the privacy of these Americans.

Questions:

- **To the best of your knowledge, what limits currently exist on the government's ability to store, analyze, and disseminate information it collects without a FISA warrant on Americans who were never a target?**
- **Should new legislation require stronger minimization procedures, either for all Americans' communications or at least for international communications that are "incidentally" collected?**

8. It appears from the text of the Protect America Act that Americans who travel abroad are now extremely vulnerable to warrantless surveillance. When Americans travel out of the country, the Act suggests that the government can wiretap them—without any warrant—as long as a significant purpose of the surveillance is to obtain foreign intelligence information.

Questions:

- **Is this correct?**
- **Can you explain what effect Executive Order 12333 has on the wiretapping of Americans abroad, and whether this Order will continue to have force under the Protect America Act?**
- **To protect the rights of Americans who travel abroad, should we require a warrant anytime the government wants to target a U.S. citizen?**

9. We spent much of the hearing debating the Protect America Act, which is very controversial and troubling in itself. But the Administration is also asking for additional changes in the FISA law. For example, Director McConnell has asked for a variety of "streamlining" measures and for an extension of FISA's emergency provision from 72 hours to one week.

Questions:

- **What do you think of these new requests?**
- **Beyond this debate we are having over FISA and the Protect America Act, what else does Congress need to do to ensure that our intelligence programs are as effective and responsible as possible?**
    - **It has been reported that the National Security Agency is having many problems with management and with the computational and translational aspects of intelligence analysis. Should these be priorities?**
- **Unfortunately, a majority of this Committee is hampered in this debate by not knowing precisely what we are fixing. Despite subpoenas, we have been denied the legal justifications for the warrantless surveillance program, and we have been denied access to the FISA court opinions that we are told made new legislation**

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00139 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.072

necessary. We are being told we need to fix a problem whose nature and scope have not been revealed to us.

- **Given the secrecy that enshrouds this entire debate, how would you recommend Congress fulfill its oversight responsibility?**
- **Do you think Congress should conduct a broader review of intelligence policy at this time?**

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00140 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.073

Senator Charles E. Schumer
Written Questions for Director of National Intelligence McConnell
October 2, 2007

1. Engineer Susan Landau, writing in the Washington *Post*, argued on August 9, 2007 that the wiretapping permitted under the Protect America Act (PAA) will create unintended information security risks for the United States. Because the executive branch still requires a warrant to acquire domestic-to-domestic communications, the National Security Agency (NSA) will need to filter these protected communications from those that can be intercepted without a warrant under the PAA. Landau states that the NSA will need to build "massive automatic surveillance capabilities into telephone switches[,]" but she warns that creating this infrastructure will mean that "within 10 years, the United States will be vulnerable to attacks from hackers across the globe, as well as the militaries of China, Russia and other nations." Thus, the same technology used by the NSA to protect Americans could potentially be used against us in a cyber-attack.

a. Do you agree with Ms. Landau's prediction that the executive branch will need to build surveillance capabilities into telephone switches?
b. If the executive branch does foresee using sweeping collection mechanisms such as Ms. Landau describes, what assurance can you give this Committee that this collection technology will not ultimately be used to attack the United States?

2. Assistant Attorney General Kenneth L. Wainstein, in a letter to Congress on September 14, 2007, reiterated the executive branch's position that a warrant is required when a U.S. person is the target of such surveillance. S. 2011, an alternative bill for modernizing the Foreign Intelligence Surveillance Act (FISA), would have directed the Attorney General to develop his or her own guidelines for obtaining a court order when communications that are acquired without a warrant evolve into a surveillance effort targeted at a U.S. person. The PAA does not direct the Attorney General to develop such consistent safeguards. Will you support adding a provision to the PAA, if it is renewed, that directs the Attorney General to develop consistent guidelines to ensure that the executive branch seeks judicial approval for continuing any electronic surveillance that effectively becomes surveillance of a U.S. person or that infringes on the reasonable expectation of privacy of a U.S. person? If not, why not?

3. You stated at the hearing on September 25, 2007, that the bulk collection of electronic communications would be authorized under the PAA, but only if the communications constitute foreign intelligence. However, another witness, Suzanne Spaulding, later stated that "as a matter of statutory interpretation, [FISA Section] 105A does not require that it have anything to do with foreign intelligence or be for foreign intelligence purposes. It simply defines all of those communications out of those statutory protections. So, it certainly would enable or not put any restrictions on the bulk collection." The application of Section 105B, in contrast, is limited to foreign intelligence information.

a. Do you wish to clarify your statements at the hearing regarding the extent to which the PAA authorizes the bulk collection of electronic communications, in light of the different language used in Sections 105A and 105B and the view expressed by Ms. Spaulding following your testimony?

53358.074

b. Please explain whether there is any operational or other reason why Section 105A refers to all surveillance directed at a person reasonably believed to be outside the United States, while Section 105B is limited to foreign intelligence.

4. The Church Committee of the 1970s, which uncovered abuses of electronic surveillance prior to the passage of FISA, noted that the "inherently intrusive nature of electronic surveillance . . . has enabled the Government to generate vast amounts of information – unrelated to any legitimate government interest – about the personal and political lives of American citizens. The collection of this type of information has, in turn, raised the danger of its use for partisan political and other improper ends by senior administration officials."

a. Does the executive branch, as a matter of practice, permanently discard, within a certain period of time, electronic communications that are acquired during surveillance but that are found not to contain foreign intelligence information? If so, for what period of time? If not, why not?
b. What assurance can you give this Committee that information collected through electronic surveillance will be safeguarded from being used for "partisan political and other improper ends" by officials in our current and future presidential administrations?

5. You have repeatedly claimed that minimization rules are sufficient to protect the privacy of U.S. persons whose communications are acquired under the new Section 105B of FISA, added by the PAA. However, public assessment of the adequacy of these rules is difficult because the minimization procedures are classified. Moreover, some observers are concerned that these rules are inconsistently applied. For example, a *Newsweek* investigation found that in just 18 months from 2004 to 2005, the NSA gave out the redacted names of 10,000 U.S. citizens to bureaucrats and analysts. During the hearing before the Judiciary Committee on September 25, 2007, you indicated that you are willing to support annual review of the minimization procedures by the Foreign Intelligence Surveillance Court and by Congress.

a. Will you support adding a provision to the PAA, if it is renewed, that requires the Foreign Intelligence Surveillance Court to review minimization rules at least annually and to issue a decision on whether the NSA's rules are constitutional and adequate to protect Americans? If not, why not?
b. Will you also support adding a provision to the PAA, if it is renewed, that requires the Foreign Intelligence Surveillance Court to review minimization rules whenever these rules are revised and to issue a decision on whether the NSA's rules are constitutional and adequate to protect Americans? If not, why not?
c. Will you also support adding a provision to the PAA, if it is renewed, that requires a periodic independent assessment of whether the intelligence community is complying with the applicable minimization rules? If not, why not?

6. Section 105A of FISA, added by the PAA, provides that FISA's warrant requirement does not apply to surveillance "directed at a person reasonably believed" to be in a foreign country. Section 105B of FISA, added by the PAA, sets out an alternative procedure for surveillance not covered by FISA, but appears to use broader terminology.

53358.075

Section 105B provides that you and the Attorney General may, on your own authority, direct the collection of intelligence information "concerning" persons reasonably believed to be in a foreign country.

a. In your interpretation of the PAA, is surveillance "concerning" an overseas person in fact a broader category than surveillance "directed at" an overseas person? Stated differently, do you read the PAA to grant you (with the Attorney General) the authority to order the collection of a broader universe of intelligence information than what is actually exempted from FISA's warrant requirement?
b. If so, please explain why you advocated for FISA modernization legislation that contains this language.

7. In his letter to Congress of September 14, 2007, Assistant Attorney General Wainstein also stated that the PAA does not authorize warrantless physical searches of the homes or effects of Americans; acquisition of domestic-to-domestic communications; or the collection of medical, library or other business records for foreign intelligence purposes. In order to provide greater clarity and given the Administration's position that the PAA already does not authorize the above activities, will you support adding a provision to the PAA, if it is renewed, that explicitly states that the PAA does not authorize warrantless physical searches of the homes or effects of Americans; acquisition of domestic-to-domestic communications; or the collection of medical, library or other business records for foreign intelligence purposes? If not, why not?

53358.076

Answers to Senator Kennedy's Questions for the Record

Question 1.

- Yes. The Fourth Amendment does apply to protect Americans from unreasonable surveillance of their communications, including international communications.

- The Protect America Act (PAA) raises significant 4th Amendment concerns because of the potential breadth of its application, which would seem to permit warrantless interception of communications between US citizens inside the United States.

- FISA judges play an essential role in safeguarding Americans' 4th Amendment rights. As Supreme Court Justice Powell wrote for the majority in the *Keith* case, "The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. ...But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."

Question 2.

The FISA court should have a discretionary role that allows it to fulfill its function as a neutral check to ensure compliance with the statutory standard, which the PAA's standard of "clearly erroneous" does not adequately provide. The Administration's argument that giving the court that role is too burdensome for the executive branch is not convincing. Even under the PAA, the government has to meet the statutory standard of having reasonable procedures in place to determine that the target is overseas. It is hard to see how giving the court a meaningful role in ensuring that the government is in fact meeting that standard significantly enhances the burden.

53358.077

Question 3.

Any enhanced surveillance authorities should be accompanied by enhanced Congressional oversight. The PAA, and even the changes proposed in the RESTORE Act and the Senate Intelligence bill, takes electronic surveillance into previously uncharted territory and it is absolutely essential that Congress more carefully monitor implementation so as to promptly and effectively reconsider the law as problems and concerns are identified.

Question 4.

It is hard to imagine a more powerful way to undermine respect for the rule of law and the critical role that communication providers play as the last line of defense against government abuse than to grant them blanket retroactive immunity for whatever they may have done to assist the warrantless surveillance of Americans. Moreover, it's not clear why this is needed. Under current law, communication providers already can avoid liability if they simply have a letter from the AG saying the government's request meets statutory requirements. If they did not even get that, what message do we send by giving them immunity for totally disregarding the statutory requirements of the law?

Moreover, granting immunity will make it harder for any company in future to say no to a request from the government for information that statutory law seems to prohibit. The government can simply assure them that they are "doing their patriotic duty" and will get immunity in the end. It is this kind of "legal limbo"-- when the government comes in with a request that does not meet statutory requirements but which the government asserts is legal anyway-- that puts companies in a position of having to second-guess the government's legal assertion. Granting immunity creates this uncertain environment. Requiring that statutory requirements be met creates the certainty that both companies and intelligence professionals need.

The Administration has argued that if blanket immunity is not granted, companies will be deterred from cooperating in the future. However, current law and the proposed House and Senate Intelligence bills all provide unequivocally that companies that cooperate with a request

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00145 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.078

from the government that meets statutory requirements will be immune from any liability going forward. Thus, the only cooperation that will be deterred is cooperation with requests that do not meet statutory requirements--and that is precisely the kind of cooperation the law is intended to deter.

In an area such as this, where the normal safeguards of transparency are lacking, requiring communication providers to at least get a certification that the government's request to assist with surveillance is legal under the statute serves as an important potential deterrent to abusive behavior by the government. At a minimum, Congress needs to fully understand what past activities would be immunized before adopting such a wide-ranging provision.

Unless the carriers engaged in unlawful activity on a very large scale, bankruptcy seems unlikely. Nevertheless, some mitigation of the amount of liability incurred by the carriers may be appropriate, given that they were apparently approached by the government at a time when Americans were still reeling from the attacks of 9/11.

Question 5.

- Director McConnell testified that the PAA would allow bulk collection, such as of all communications from overseas to people in the US, without a warrant. More careful statutory language requiring more particularity in an application to the court in advance of collection, even if only for approval of a program of surveillance directed at a group rather than specific individuals, could help address this problem. For example, Congress could require that the government make some showing to the court of the reasonableness of their claim that this is designed to collect foreign intelligence. Presumably only a very small percentage of Americans' international communications relate in any way to legitimate foreign intelligence requirements, so bulk collection would have a hard time meeting that standard.

- Section 105B provides authority for the AG and DNI to collect intelligence information inside the United States so long as (1) the information is about a person who happens to be outside the US at the time--including, of course, a US citizen, (2) the collection of that information does not involve electronic surveillance, and (3) the government requires the

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00146 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.079

assistance of someone with access to a communication or communication equipment. It appears to be about electronic surveillance targeting someone outside the US (which is now no long considered "electronic surveillance"), but it in fact provides authorization for the government to gather any kind of communication and to gather it inside the United States. Thus, it would appear to authorize intercepting US mail between two people inside the United States, so long as the government reasonably believes the letter discusses, at least in part, someone outside the US. The careful legal regime governing mail intercepts is overruled by the "notwithstanding any other law" language" in section 105B.

Moreover, it would appear that the AG could authorize the physical search of your home to find a letter from your son overseas or the family computer on which you've stored his emails, although this would raise significant 4th Amendment issues. The FISA provisions that regulate physical searches become irrelevant because section 105B applies "notwithstanding any other law."

Similarly, the protections that Congress worked so hard to enact last year for section 215, the so-called business records provision, would also appear to be overruled under circumstances in which Section 105B applies. Thus, any individual who can help the government obtain access to communications that involve someone outside the United States can now be compelled to provide that assistance under section 105B, with fewer safeguards.

- The government has not publicly provided a reason for using the significantly broader term "concerning" rather than "directed at" or "targeting." In fact, Director McConnell testified that the author of that phrase in the bill did not have any reason for using that term and the DNI suggested that a change might be appropriate.

- The PAA makes significant changes in the legal framework under which electronic surveillance has been conducted in this country for nearly 30 years.

53358.080

Question 6.

- FISA was carefully crafted so as not to unduly hamper foreign intelligence collection that was clearly focused on foreign targets overseas. However, FISA has always covered international communications of Americans over the wires if collected inside the United States, even when the US-end was not the target. (see FISA Section 101(f)(2).)

- No. One of the things that has changed dramatically since FISA was first enacted is that far more Americans are engaged far more international communications, particularly with the widespread use of email. Thus, collection of Americans' international communications raises significantly greater privacy concerns today than it did in 1978.

Question 7.

While the PAA provides that information gathered under 105B must be subjected to minimization procedures, it appears that the statutory requirements that apply are the less rigorous procedures that apply when a FISA judge has reviewed a full FISA application and found probable cause to believe that the target of the surveillance was a foreign power or agent of a foreign power.

The Protect Act simply refers to "the minimization procedures in section 101(h)." There are two sets of minimization procedures proscribed in that section. The first set applies when a FISA judge has approved an application. The second set is much more stringent and applies when the Attorney General has approved surveillance without going to a FISA judge. These more rigorous procedures are statutorily limited to situations in which the AG is acting pursuant to the authority granted him in section 102(a). Thus, they would not apply to the unilateral authority granted to the AG and DNI in the Protect Act.

The general minimization procedures in 101(h)(1)-(3) reflect a recognition that, even after all the application requirements had been met and approved by a FISA judge, there remains some risk that information about U.S. persons (USPs) might be collected. These procedures require steps be taken to minimize the acquisition and retention, and prohibit the dissemination, of such information. However, the procedures are to be "reasonably designed in light of the

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00148 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.081

purpose and technique" of the surveillance and "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." This is a very broad and flexible standard, particularly given the current scope of "foreign intelligence."

Under section 101(h)(4), if surveillance is conducted pursuant to AG authorization rather than a warrant from a FISA judge—a situation more analogous to the 105B authority in the PAA-- no contents of any communication to which a USP is a party can be disclosed, disseminated, or used for any purpose or retained for more than 72 hours without getting a court order, unless the AG determines that the information indicates a threat of death or serious bodily harm. Concern about ensuring that electronic surveillance authorized unilaterally by the AG could not be used to gather information about USPs was so strong when FISA was enacted that even the mere existence of such a communication was included in this restriction. At a minimum, this stricter procedure should have applied to information collected under section 105B of the PAA. With a more carefully constructed program, such as provided for in the RESTORE Act, minimization that limits dissemination to information that is related to an attack on the United States or other significant national security threats would be appropriate.

Question 8.

The statutory language of the PAA would appear to allow warrantless surveillance targeting Americans who are traveling overseas even if their communications are collected inside the United States. Executive Order 12333, section 2.5, authorizes the Attorney General to approve surveillance of Americans abroad only if he decides there is probable cause to believe the surveillance is directed against a foreign power or an agent of a foreign power. This is not directly affected by the PAA but it can be changed at any time by the President, acting unilaterally. In order to more appropriately protect the privacy rights of U.S. persons overseas, Congress should require a FISA warrant to target Americans overseas when the collection takes place inside the United States. Collection that takes place overseas may be more difficult to treat in the same manner, particularly given that espionage overseas almost inevitably violates the laws of the country in which it takes place. The FISA court may not be comfortable authorizing such activity. However, at a minimum, Congress could codify the requirement that the Attorney

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00149 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.082

General make a finding of probable cause to believe that the American target is an agent of a foreign power. This could include reporting requirements and IG audits.

Question 9.

Any changes requested by the Administration to other provisions of FISA should only be made with a full understanding of the consequences, after a clear showing by the executive branch that they are necessary to meet national security imperatives and the objectives cannot be accomplished in a less intrusive way, and should be crafted as narrowly as possible.

Rather than attempt to guess at what might really be needed to meet today's challenges and how these and other changes will affect our ability to meet those challenges and protect Americans' privacy, Congress should take the time to ensure they understand the full context in which these changes are being sought. This includes the problems that have prompted them, particularly as these relate to current and past intelligence activities and the changing nature of the threat, as well as how these new authorities, definitions, and procedures would relate to all of the other national security and law enforcement tools available to the government.

I urge Congress not to consider any "overhaul" of FISA without first undertaking a comprehensive review of domestic intelligence collection. The attacks of 9/11 revealed a vulnerability at home that led to a dramatic increase in domestic intelligence activity. The Federal Bureau of Investigation's priorities were dramatically altered, as it was pressed to place domestic intelligence collection at the forefront rather than criminal law enforcement. But the FBI is not the only entity engaged in domestic intelligence. The Central Intelligence Agency, National Security Agency, Department of Defense, Department of Homeland Security, and state and local law enforcement are among the many entities gathering intelligence inside the US. The threat to the homeland presents unique challenges, both to effective intelligence and to appropriate protections against unwarranted government intrusion.

Unfortunately, the legal framework governing this intelligence activity has come to resemble a Rube Goldberg contraption rather than the coherent foundation we expect and need from our laws. The rules that govern domestic intelligence collection are scattered throughout the US Code and a multitude of internal agency policies, guidelines, and directives, developed

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00150 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.083

piecemeal over time, often adopted quickly in response to scandal or crisis and sometimes in secret.

Rather than continuing this pattern, Congress should consider establishing a Joint Inquiry or Task Force with representation from the most relevant committees (Intelligence, Judiciary, Armed Services, Foreign Affairs, and Homeland Security), to carefully examine the nature of the threat inside the US and the most effective strategies for countering it. Then this task force, the entire Congress, and the American public, can consider whether we have the appropriate institutional and legal framework for ensuring that we have the intelligence necessary to implement those strategies, with adequate safeguards and oversight.

The various authorities for gathering information inside the United States, including the authorities in FISA, need to be considered and understood in relation to each other, not in isolation. For example, Congress needs to understand how broader FISA authority relates to the various current authorities for obtaining or reviewing records, such as national security letters, section 215 of FISA, and the physical search pen register/trap and trace authorities in FISA, and the counterparts to these in the criminal context, as well as other law enforcement tools such as grand juries and material witness statutes.

Executive Order 12333, echoed in FISA, calls for using the "least intrusive collection techniques feasible." The appropriateness of using electronic surveillance or other intrusive techniques to gather the communications of Americans should be considered in light of other, less intrusive techniques that might be available to establish, for example, whether a phone number belongs to a suspected terrorist or the pizza delivery shop. It's not the "all or nothing" proposition often portrayed in some of the debates.

Congress should undertake this comprehensive consideration of domestic intelligence with an eye toward the future but informed by the past and present. Until Congress fully understands precisely what has and is being done in terms of the collection and exploitation of intelligence related to activities inside the US, by all national security agencies, it cannot wisely anticipate the needs and potential problems going forward.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00151 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.084

This applies particularly to changes to FISA. Congress must be certain that it has been fully informed about the details of the Terrorist Surveillance Program and any other surveillance programs or activities initiated after 9/11, not just in their current form but in the very earliest stages, including the legal justifications offered at the time the activities were initiated. Understanding how the law operates in times of crisis and stress is key to understanding how it might need to be strengthened or adjusted to meet national security imperatives in ways that will protect against future abuse.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00152 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.085

SUBMISSIONS FOR THE RECORD

Testimony of James A. Baker

Before the

Committee on the Judiciary

United States Senate

September 25, 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

53358.086

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

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00154 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.087

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

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00155 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.088

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. 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

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00156 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.089

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

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00157 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.090

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

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00158 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.091

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.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00159 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.092

KEEPING THE FISA BALANCE. PROTECTING US FROM ATTACK

Statement of

H. BRYAN CUNNINGHAM[1]

PRINCIPAL, MORGAN & CUNNINGHAM LLC
www.morgancunningham.net

Former CIA Assistant General Counsel and Federal Prosecutor (1994-2000)
Deputy Legal Adviser to the National Security Council (2002-2004)
Information Security and Privacy Lawyer (2004-Present)

before the

UNITED STATES SENATE COMMITTEE ON THE JUDICIARY

On the subject of

"STRENGTHENING FISA: DOES THE PROTECT AMERICA ACT PROTECT AMERICANS' CIVIL LIBERTIES AND ENHANCE SECURITY?"

September 25, 2007

Mr. Chairman, Ranking Member Specter, and Members of the Committee, thank you for inviting me to testify again before this Committee on one of the most important national security challenges facing our Nation. Shortly after disclosure of the Terrorist Surveillance Program, I co-authored, with former senior Democratic homeland security staff member Dan Prieto, an Op-Ed entitled "The Eavesdropping Debate We Should Be Having" (http://www.ksg.harvard.edu/ksgnews/Features/opeds/020506_prieto.htm). We called for three touchstones for foreign intelligence surveillance: (1) updating FISA to achieve its original national security and civil liberties goals, but adjusting the badly outdated law to the revolutionary technological since 1978 so that our intelligence officers can protect us from attack; (2) ensuring that equally strong civil liberties protections, though perhaps different from those envisioned in 1978, are built into any such changes; and (3) continuing a meaningful role for our Courts to the extent consistent with our Constitution and national security.

The Protect America Act (PAA), passed by Congress last month, met these three goals to a significant degree, at least in the area of collection of intelligence from foreign-to-foreign communications. This hearing, and others that have preceded it, are an important part of that debate we recommended 19 months ago and I commend this Committee for furthering it.

As a recovering career government attorney and intelligence officer (having served six years in the Clinton Administration and two years in the George W. Bush Administration), I will do my best to resist the temptation to slip into a legalistic discussion of the minutae of the Foreign Intelligence Surveillance Act or the related constitutional issues. To assist this Committee, of course, our panel likely will have to get into these some of these details today, but first I would like to take a step back. Unfortunately, some of the loudest voices in this debate over the past few weeks have generated far more heat than light. There has been a great deal of misunderstanding, if not misinformation, in the public discussion, and I hope we can today dispel some of the myths that have arisen since Congress passed the PAA.

I would like to provide a couple of observations and offer several recommendations and I will be pleased to respond to any questions the Committee may have, or to provide additional information as the Committee may request.

The FISA Balance

For the first two centuries of our Nation's history, our courts uniformly recognized that our Constitution assigned to the Executive Branch of our government, and specifically the President, the "plenary" authority over the conduct of our foreign affairs.[2] For example, in *Department of the Navy v. Egan,* Justice Harry Blackmun, writing for the majority, reiterated that the "Court . . . has recognized 'the generally accepted view that foreign policy was the province and responsibility of the Executive.'"[3] More to the point, Justice O'Connor stated in 1988 that the Executive Branch's authority to conduct intelligence operations "lie[s] *at the core of* "the very delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations."[4]

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00161 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.094

Prior to 1978, all presidents, of both political parties, at least since Franklin Roosevelt, conducted significant programs of foreign intelligence electronic surveillance, here and abroad, targeted against Americans and foreigners, without warrants or other court involvement. Federal appellate courts repeatedly upheld the constitutionality of such warrantless surveillance.[5] To cite one example, the Fifth Circuit Court of Appeals, in *United States v. Brown*, upheld the President's inherent constitutional authority to authorize warrantless wiretaps for foreign intelligence purposes, explaining that:

> [B]ecause of the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs, *we reaffirm. . . that the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence. Restrictions upon the President's power which are appropriate in cases of domestic security become artificial in the context of the international sphere.* Our holding . . . is buttressed by a thread which runs through the Federalist Papers: that the President must take care to safeguard the nation from possible foreign encroachment, whether in its existence as a nation or in its intercourse with other nations.[6]

Following revelations about real "domestic spying" (in stark contrast to what we are discussing today which, based on United States Supreme Court and other federal court precedent, is *foreign* intelligence collection) in previous decades, in the late 1970s Congress and Administrations of two presidents of different political parties set out to regulate – by statute – electronic surveillance for foreign intelligence purposes. During the lengthy deliberations preceding passage of that statute, both the Executive Branch and the FISA Congress itself, in legislative history, made clear that the passage of FISA did *not* mean either that: (1) the Constitution required the precise requirements enacted in FISA for foreign intelligence surveillance; or (2) that the Supreme Court would conclude that Congress could constitutionally bind the President to those requirements in all cases.

As recent testimony to Congress has made abundantly clear, and as the FISA Congress legislative history confirms, the balance that was struck by the 1978 Congress between protecting Americans' vital civil liberties from undue government intrusion and the equally vital responsibility to protect our people from foreign threats was essentially this: Court-issued warrants should be required to conduct electronic surveillance targeted or directed at United States Persons (citizens or Permanent Resident Aliens) located *inside* the United States. No such warrants, or, indeed, even court involvement, should be required to conduct such surveillance targeted or directed against individuals (including US Persons) located *outside* the United States.

The 1978 Congress quite clearly *did not intend* that warrants be required for electronic surveillance targeted against persons located outside the United States. This is evident not only from the definitions of "electronic surveillance" in FISA itself, but also from the 1978 FISA legislative history.[7]

I believe that most on both sides of the political aisle today believe that, generally speaking, this is the proper balance, assuming it remains technologically possible to observe these lines of demarcation, which is increasingly doubtful. As an aside, as has been discussed

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00162 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.095

publicly by technically and legally knowledgeable experts, there are a host of technological developments which have rendered the original FISA unworkable against post-9/11 threats to our Nation, including the development of "packet-based" communications, the use of proxy servers and Internet-based, encrypted, highly mobile telephone communications and PDAs, the increasingly distant relationship between IP addresses and real-time, actual physical location, and the routing of vast amounts of purely overseas Internet communications through the United States.[8] One key problem remains the difficulty, given today's technology, to determine *before the fact* who the bad guys are, where they are located, and where the bad guys they are calling are located. To cite one specific example, as Director of National Intelligence McConnell testified last week, and common sense dictates, it is today, in many cases, *impossible* to make a determination, in advance of initiating electronic surveillance, whether the communications of an overseas target will be purely foreign-to-foreign.

In order to put this balance into our law, the 1978 FISA Congress chose a set of understandable but, in hindsight, mistaken factors to try and carve out foreign-to-foreign communications from the law's requirements. For purposes of discussion of the PAA, the key factors in the original FISA were: (1) place of collection (whether inside the United States or overseas); and (2) method of communications (whether by "wire" or by "radio"). In 1978, the vast majority of domestic communications were carried, literally, by wire, whereas the vast majority of overseas communications of interest to our intelligence community were carried by "radio," including by satellite. Thus, it made sense in 1978 to apply FISA's strict requirements principally to wire communications but *not* to "radio" communications. Clearly demonstrating Congress' intent to exempt from FISA's coverage collection of foreign-to-foreign communications *even when the collection was conducted inside the United States*, the law only applied its strict requirements to collection against radio communications "if both the sender and all intended recipients are located within the United States" (or, of course, if the communications of a particular, known US Person located in the United States were intentionally targeted).[9]

The key historical point, seemingly lost in much of the debate, is this: selection of these statutory criteria were the means to an end, not an end in themselves. And the means no longer further the original end. This is because, gradually over the three decades since FISA was passed, the 1978 communications technology situation reversed itself. Today, a significant percentage of truly domestic U.S. communications are carried by "radio," cellular and microwave transmissions, while most international communications now are carried by "wire," that is, fiberoptic cables.

As a result, prior to the PAA, as one FISA Court judge reportedly ruled earlier this year, FISA had morphed far beyond the intent of Congress to require a warrant even for communications between two foreigners both overseas so long as the collection happened to occur in the United States. This clearly was not the balance that the 1978 Congress intended to strike.

Part of the bargain that the 1978 Congress understood, as have all subsequent Congresses under the control of both political parties, was that electronic surveillance of foreign-to-foreign communications, and, indeed, some communications between targets abroad and the United States, would be carried out with no warrant and no judicial involvement whatsoever. Such

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00163 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.096

surveillance was carried out effectively, and consistent with the Fourth Amendment, for nearly three decades, under Executive Orders and strictly enforced procedures required by those orders. Also understood by the 1978 Congress, and all subsequent Congresses, was that, in the course of targeting the communications of foreigners abroad, our government would necessarily also collect a significant amount of communications of individuals in the United States with whom the overseas targets were communicating. Fourth Amendment protection for Americans under these circumstances was achieved by a panoply of strict requirements, including: Attorney General approval for collection, though overseas, targeting US Persons abroad, careful training, monitoring, and oversight; strict limitations on sharing and use of such information; and, perhaps most important, strictly enforced minimization requirements for information related to US Persons.

Through these minimization requirements, as with domestic criminal wiretaps, information not targeted for collection and not meeting the criteria of information authorized for collection ("foreign intelligence" in the case of foreign intelligence collection), or mistakenly collected, generally could not be shared, used, or retained by the government. Based on recent testimony, it appears that equivalent protections are in place or being developed for information to be collected under the PAA. Under the PAA, however, unlike during the past three decades, there is some FISA Court oversight of the procedures under which such collection is undertaken, as well as enhanced Congressional oversight.

To be clear: US Government electronic surveillance of foreign-to-foreign communications outside of FISA has been conducted for decades, even though it has been well understood that communications of individuals located inside the United States would be collected – *without a warrant or court involvement* -- "inadvertently," where an overseas person, not the person here, was targeted. This is not new and it is precisely the situation that appears to pertain after passage of the PAA.

Rewriting the Bargain

Although I do not know the facts, and they may be classified, it is possible that the PAA's removal of the "place of collection" limitation under FISA will increase the amount of "inadvertent," non-targeted collection of communications of persons located in the United States communicating with targeted suspected terrorists overseas or other foreign intelligence collection targets. The PAA, by its explicit terms, however, *only* modifies the warrant requirement for electronic surveillance targeted against persons "reasonably believed to be located outside the United States," and the law contains not a word about electronic surveillance targeted against persons located here. Nonetheless, PAA opponents have repeatedly asserted that "millions" or "billions" of communications of persons located here will now be collected that were not collected prior to the PAA. Since, as discussed above, the same *types* of communications involving persons inside the United States have been inadvertently collected for decades under only Executive Orders, and in the absence of any other plausible explanation, I can only guess that it is an assumption of additional *volume* of such communications given the removal of the place-of-collection restriction that has led to such charges.

53358.097

If this is in fact a principal objection of the PAA's opponents, it may be a legitimate issue for debate, but opponents should straightforwardly explain what they are attempting to do: they are attempting to rewrite the bargain, to upset the balance, struck by the 1978 FISA Congress. That "bargain" was, again, to require warrants for electronic surveillance targeted against persons in the United States and not for those outside it. Place and type of collection limitations were nothing more or less than the means to enforce that bargain. If opponents want to argue that the American people should rewrite that bargain, should undo the balance struck decades ago under continuing threat of catastrophic foreign attack, they should say so. That may be a legitimate debate. It is not, in my view, legitimate or helpful to suggest, as many have, that somehow the government is grabbing sweeping new powers to "spy on" Americans at home. Quite the opposite. What the PAA really did was to carry forward the bargain, to restore the balance between civil liberties and protection from attack so carefully struck in 1978. If we want to reconsider that balance in wartime, Congress should least be clear that that is what it is doing.

Public Confidence, Unintended Consequences, and Clearing Smoke

Viewing the Protect America Act in its proper context, however, is not to say that it cannot be improved upon. There are a number of measures which, while not, in my view, constitutionally necessary, could increase congressional and public confidence, provide permanent, clear guidance to the civil servants carrying out intelligence collection, and increase the effectiveness of whatever program ultimately is made permanent. In addition to the proposals discussed at the end of my testimony, areas where improvements potentially could be made include:

- More clearly defining, and possibly strengthening, the role of the Foreign Intelligence Surveillance Court, in approving, and supervising the use of, the criteria and parameters for PAA-authorized collection;

- Providing more comprehensive immunity for private sector communications service providers assisting the government in carrying out electronic surveillance activities where those providers are informed, in writing, of the lawful authority under which they are asked to act; and

- Clarifying, whether in statute or legislative history, the definitions of some of the terms used in the Protect America Act, potentially including "targeted," "directed," and "concerning"

Such changes, however, should only be made after careful consideration of their potential unintended consequences, and specific language should be proposed early in the process to give all sides time to fully understand its implications. Further, any such changes must take into account all legitimate needs, arguments, and explanations of those technically expert in the area and, critically, those who must carry out the law's requirements, even if some of those arguments and explanations may not be discussed publicly. Finally, and most importantly, any changes must be made in light of cold, clear facts and a realistic understanding of the history and constitutional status of electronic surveillance in the United States, and of the original FISA. Decisions should not be made based on misleading, false, or speculative

53358.098

arguments, about, for example, "billions" of new communications of individuals in the United States, or "domestic spying," or be based on partisan political battles or ill will between the current Congress and the current Administration. After all, if Congress gets it right, the new methods for carrying forward the old balance will likely stand for many years, and will almost certainly be used far more by future presidents, of both political parties, than by the current one.

Private Sector Cooperation and Risk Aversion

Once again, I want to commend the Chairman and Senator Specter and those in Congress attempting to foster a sober, fact-based debate on how to strike the right balance between protecting against attack and safeguarding our civil liberties. As I argued in my 2006 Op-Ed, Congress is the appropriate place for this debate and I am pleased to be a part of it, along with the other members of this panel. The debate must be thorough and vigorous. But, in my view, it should be fought here, in Congress.

Unfortunately, it is being fought in our courts and the media as well and, to dramatically understate the problem, not always based on accurate information. Recent government testimony indicates that FISA modernization opponents, because they object to the government's actions, have filed more than 40 civil lawsuits including, disturbingly, against communications providers alleged to have assisted the government in conducting electronic surveillance activities, even where the government allegedly assured such providers that requests for assistance were lawful and constitutional. Political differences about activities to protect our Nation from attack should not be fought through proxy attacks on companies simply trying to assist in defending our country. Providers should be able to rely on assurances from their government and should not be retroactively saddled with economically punishing litigation as a way to try and prevent them from cooperating with the government.

Such attacks are bad public policy. Speaking as a private lawyer advising companies on their interaction with the government, I believe that attempting to settle political or policy differences through such proxy lawsuits succeeds only in creating uncertainty and a reluctance on the part of the private sector to cooperate with the government, even where the law is clear. I also, frankly, think it is fundamentally unfair, if not immoral, to try, through litigation punishing those cooperating with the government, to intimidate service providers and, thereby, win political fights that rightfully belong in Congress.

Multiple bipartisan investigations criticized, appropriately in my view, both the Clinton and Bush Administrations for risk aversion by multiple intelligence agencies, and for failing to utilize their full legal authorities to collect intelligence, including through wiretapping, concerning communications between terrorists overseas and their confederates here in the United States.[10] Having spent a number of years in the Clinton Administration as CIA Assistant General Counsel advising career officers conducting risky intelligence operations, I saw firsthand how well-founded fears of career-ending investigations and after-the-fact legal and rule changes led dedicated officers to fail to take clearly lawful and proper actions to collect intelligence. This risk aversion, which crippled our Nation before 9/11, is, I fear, returning to the ranks of our career civil servants in the intelligence and law-enforcement officers.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00166 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.099

Legitimate oversight is a necessary and vital part of our democratic system and, of course, intentional illegal activity must be discovered and punished. But our career intelligence officers – and, make no mistake, *these* are the people, not the President, the Vice President, or other political appointees, who must carry forward whatever vital reforms Congress enacts – must not be put into the position of attempting to do their duty under the constant fear of being punished for following rules that have been changed. Among other things, this means putting into place legal rules that are: (1) clear and easy to follow; and (2) stable over some reasonable period of time. In short, government by sunset cannot become the norm in the regulation of intelligence activities to protect our country from attack. Our career officers need to know that the rules will be the same next year as this year, absent significant changes in technology, threats, or other compelling conditions.

In addition to doing right by our career officers and reducing risk aversion, stable legal rules over a reasonable period of time are the only workable solution. Each time the law changes significantly, policies, regulations, other guidance must change, and, perhaps most importantly, massive changes must be made to numerous and comprehensive training programs in order to reeducate generations of officers conducting intelligence activities. Whatever Congress does next in the vital area of FISA modernization, I urge you to satisfy yourselves with the balance struck sufficiently to make those changes permanent. Wherever the political blame may fall, six-month sunsets are bad for morale, bad for the risk taking necessary for successful intelligence collection, and dangerous to our ability to protect our Nation from attack.

Potential Solutions Beyond the Protect America Act

As noted above, the PAA, whether one supports it as passed or not, only solves one of the myriad problems created by technological change and the language of the original FISA. Other challenges which, in my view, require urgent attention, include: collection of information originally sought under the Terrorist Surveillance Program; collecting foreign intelligence in situations where there is literally not time to get any new advance approval without missing critical threat information, or no way to timely determine place of collection, location, or nationality of the targeted individual; and protecting privacy and civil liberties when information collected with electronic surveillance and other highly intrusive techniques is shared across entities and governments. These challenges, in my view, can only be addressed adequately by some combination of the approaches discussed below. These approaches also, in my judgment, can help improve the PAA, and its implementation going forward.

Programmatic Judicial Review and Approval

In our February 5, 2006, Op-Ed, Daniel Prieto and I recommended that Congress and the President, in modernizing FISA:

> *Ensure a role for the courts.* To preserve and promote appropriate judicial oversight, new methods of court involvement must be considered. As one example, courts could pre-approve categories of electronic surveillance. This would allow the government to apply strict, pre-determined criteria to particular communications without the need for case-by-

case court approvals. Categories, criteria and eavesdropping activity would be subject to regular re-examination, with approvals subject to periodic court renewals.

S. 2453, proposed in 2006, would have created clear jurisdiction for the Foreign Intelligence Surveillance Court (FISC) to conduct just such "programmatic" review. As such, I supported that legislation, even for targeted collection of international terrorism-related communications. Though I do not believe such judicial involvement to be constitutionally required, at least for communications targeted at persons located overseas, Congress should examine – based on independent expert factual analysis – whether our ability to timely determine location has become so weak that location can no longer be a meaningful factor in most cases. If that is so, as has been suggested by many experts, programmatic review, regardless of location, merits much more consideration.

Such review would provide meaningful judicial oversight, likely consistent with the Fourth Amendment for foreign intelligence-related surveillance, while redressing what I believe to be one of the fatal flaws of the 1978-era FISA in today's world, namely the requirement for individualized, target-by-target approval, based on known facts which often, in the post-9/11 world, will be *unknown* in any timely fashion, and perhaps *unknowable* given the technology and enemies we now face.

Any legislative mandate for such "programmatic approval" by courts, however, should consider whether specifically articulated criteria for the application for, and granting of, applications for programmatic surveillance orders might be useful. Any such legislation should include a clear explanation, probably in legislative history, of Congress' views as to how the articulated criteria, if met, satisfy the requirements of the Fourth Amendment.

Machine Triage/Electronic Tracking

In my view, we urgently need a recognition in law, with concomitant adjustments in the law, that the vast majority of the government's "surveillance" in the future will (if it does not already) actually consist of what I call "machine triage," that is, review of data by computers and selection of information for review by humans based on selection criteria meeting legal standards appropriate to protect our civil liberties. S. 2453, in the previous Congress, recognized the concept of "electronic tracking," as "the acquisition by an electronic, mechanical, or other surveillance *device*"[11] of certain electronic communications. The draft legislation appeared to recognize such tracking as an integral part of an electronic surveillance program eventually leading to access by *human beings* to a far smaller number of selected communications than those triaged by computer. This distinction, between information "seen," or processed only by machine, and information reviewed by a human government is, in my judgment, crucial, and as technology continues to evolve, one with which our electronic surveillance laws must grapple.

I believe that the use of machines to triage communications content and other sensitive, i.e., personally identifiable, information prior to human review will be crucial over the coming years in balancing privacy and civil liberties and our national security. Depending upon one's interpretation of the current FISA, such "machine triage" – the use of which bi-partisan experts, including the Markle Commission Task Force, have recommended – might today still require

53358.101

individual FISA applications. Such a situation, obviously, would present an insurmountable obstacle to the use of machine triage that could *enhance* civil liberties *and* operational capabilities by reducing dramatically the volume of information that must be reviewed by our perennially resource-starved intelligence agencies.

Technology to Improve Our Ability to Prevent Attacks While Enhancing Civil Liberties

As has been widely discussed, by Markle and others, currently available technologies can dramatically enhance both the government's ability to utilize increasingly large amounts of data and do so in a way that better protects our privacy and civil liberties. Congress took a significant step forward on this front in the recently signed bill to enact the 9/11 Commission's recommendations. In that new law, Congress mandated that the Executive Branch build into the emerging Information Sharing Environment technologies, available today, that:

- permit analysts to collaborate both independently and in a group (commonly known as "collective and noncollective collaboration"), and across multiple levels of national security information and controlled unclassified information;
- provide a resolution process that enables changes by authorized officials regarding rules and policies for the access, use, and retention of information within the scope of the information sharing environment; and
- incorporate continuous, real-time, and immutable audit capabilities, to the maximum extent practicable.[12]

As these new legal requirements begin to be met, as they can be with current technology, privacy and civil liberties protections not technologically possible several years ago can become routine parts of our government's activities. Equally important, as analysts and operators become far more productive, collaborative and, hopefully, effective at their missions, it may become possible for the government to do far more with far less information.

Conclusion

Today continues a vitally necessary debate, in the place where it should occur, the United States Congress. The PAA, while capable of improvement, is an important step forward in protecting our country while modernizing our privacy and civil liberties protections, and should be made permanent. Modernization reforms, however, must also take place in other areas of foreign intelligence collection, along the lines, and utilizing available technologies to achieve the new legal requirements, discussed herein. I remain confident that the appropriate balance between protecting our Nation from attack and guarding our privacy and civil liberties can, and will, be struck, so long as our career officials remain able to do their jobs and leaders on all sides of the debate go forward expeditiously, based on accurate information, and in good faith. I thank the Committee for inviting me to be part of that debate.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00169 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.102

[1] As additional relevant experience, I am currently a Principal at the Denver law firm of Morgan & Cunningham LLC, practicing primarily in the areas of information security and privacy. www.morgancunningham.net I was a founding vice-chair of the ABA CyberSecurity Privacy Task Force, and, in January 2005, was awarded the National Intelligence Medal of Achievement for work on information issues. I serve on the National Academies of Science Committee on Biodefense Analysis and Countermeasures and am a member of the Markle Foundation Task Force on National Security in the Information Age. The views expressed in my testimony are entirely my own.

[2] "The preservation of our territorial integrity and the protection of our foreign interests is intrusted, in the first instance, to the President. The Constitution, established by the people of the United States as the fundamental law of the land, has conferred upon the President the executive power; has made him the Commander in Chief of the Army and Navy; has authorized him, by and with the consent of the Senate, to make treaties, and to appoint ambassadors, public ministers, and consuls; and has made it his duty to take care that the laws be faithfully executed. In the protection of these fundamental rights, which are based upon the Constitution and grow out of the jurisdiction of this nation over its own territory and its international rights and obligations as a distinct sovereignty, the President is not limited to the enforcement of specific acts of Congress. He takes a solemn oath to faithfully execute the office of President, and to preserve, protect, and defend the Constitution of the United States. To do this he must preserve, protect, and defend those fundamental rights which flow from the Constitution itself and belong to the sovereignty it created. 22 U.S. Op. Atty. Gen. 13, 25-26, *Foreign Cables*, (1898) (citing, *inter alia*, *Cunningham v Neagle*, 135 U.S. 1 (1890) (emphasis added). Indeed, the founders of our republic specifically recognized the primary position of the President in the field of foreign affairs. For an excellent discussion of this history, *see* Powell, H. Jefferson, *The Founders and the President's Authority over Foreign Affairs*. William & Mary Law Review, Vol. 40, pp. 1471-1537 (May 1999).

[3] 484 US 518, 527, 530 (1988).

[4] *Webster v. Doe*, 486 U.S. 592, 605-06 (1988) (O'Connor, J., concurring in part, dissenting in part) (emphasis added) (*citing* prior Supreme Court decisions in *United States v. Curtiss-Wright Export Corp.*, *Department of Navy v. Egan*, and *Totten v. United States*, 92 U.S. 105 (1876)). A number of key United States appellate court decisions confirming this view specifically in the context of foreign intelligence electronic surveillance are discussed in my February 3, 2006 letter to this Committee entitled *Additional Constitutional Authorities Relevant to NSA Electronic Surveillance of International Terrorist Communications* and in *amicus* briefs I co-authored with the Washington Legal Foundation, in litigation challenging the TSP in the Eastern District of Michigan and the Court of Appeals for the Sixth Circuit. All are available at www.morgancunningham.net.

[5] For one of the most thorough and scholarly publicly available discussions of the constitutionality of warrantless electronic surveillance for foreign intelligence purposes, as well as the law of national security surveillance more generally, *see* David Kris and Doug Wilson, *National Security Investigations and Prosecutions* (West 2007). The authors explain: "every court of appeals to consider the question concluded that the President has constitutional authority to conduct warrantless electronic surveillance of foreign powers and their agents *in the United States*; the same result would seem to apply, *a fortiori*, to surveillance abroad, where Fourth Amendment protections for U.S. persons are certainly no stronger than they are in this country." *Id.* at 16-3 (emphasis added).

[6] 484 F.2d 418, 426 (5th Cir. 1973) (emphasis added) (citations omitted); *Accord United States v. Butenko*, 494 F.2d 593, 603 (3d Cir. 1974), (noting that while the "Constitution contains no express provision authorizing the President to conduct surveillance . . . it would appear that such power is . . . implied from his duty to conduct the nation's foreign affairs"). Similarly, in *United States v. Truong Dinh Hung*, a case cited with approval in 2002 by the Foreign Intelligence Surveillance Court of Review, the Court of Appeals for the Fourth Circuit, in approving warrantless electronic surveillance for foreign intelligence purposes, stated the matter plainly:

> Perhaps most crucially, the executive branch . . . is . . . constitutionally designated as the pre-eminent authority in foreign affairs . . . . Just as the separation of powers in *Keith* forced the executive to recognize a judicial role when the President conducts domestic surveillance, so the separation of powers requires us to acknowledge the *principal responsibility of the President for foreign affairs and concomitantly for foreign intelligence surveillance.*

629 F.2d 908 (4th Cir. 1980) (emphasis added) (citations omitted).

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00170 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.103

The passage of FISA, and the passage of years since, in no way undermine the reasoning of the *Brown* court, and other authorities cited herein, as to the constitutional and practical reasoning for Presidential primacy in this area.

[7] For example, the House Permanent Select Committee on Intelligence (HPSCI) report on FISA stated that the committee had "explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillance." H.R. Rep. No. 95-1283, pt. 1, at 22 (1978). Similarly, FISA's drafters made clear that the so-called "residual definition," intended to encompass types of electronic surveillance for which FISA's warrant requirement would apply, but which were not captured by the more specific definitions, was "not meant to include . . . the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States." *Id.* at 52.

[8] *See, e.g.,* testimony and writings of Kim Taipale particularly his June 19, 2006 testimony before the House Permanent Select Committee on Intelligence.

[9] 50 U.S.C. section 1801(f)(3) and (f)(1)

[10] *See, e.g., Report of the Joint Inquiry Into the Terrorist Attacks of September 11,* 2001, at p.39

[11] Emphasis added.

[12] *Improving America's Security Act* of 2007, Section 112(2). This same statute also mandates a report by the Executive Branch to Congress on the feasibility of

> (C) replacing the standards described in subparagraph (B) with a standard that would allow mission-based or threat-based permission to access or share information within the scope of the information sharing environment for a particular purpose that the Federal Government, through an appropriate process, has determined to be lawfully permissible for a particular agency, component, or employee (commonly known as an `authorized use' standard); and (D) the use of anonymized data by Federal departments, agencies, or components collecting, possessing, disseminating, or handling information within the scope of the information sharing environment, in any cases in which--
>
> > `(i) the use of such information is reasonably expected to produce results materially equivalent to the use of information that is transferred or stored in a non-anonymized form; and
> > `(ii) such use is consistent with any mission of that department, agency, or component (including any mission under a Federal statute or directive of the President) that involves the storage, retention, sharing, or exchange of personally identifiable information."

Id at Section 112(1)(j). The policies and technologies discussed in these provisions also can significantly assist the government in establishing the proper balance between national security and privacy and civil liberties.

53358.104

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

before the
Senate Committee on the Judiciary

Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?

September 25, 2007

Chairman Leahy, Ranking Member Sen. Specter, 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, but a means to compel service provider cooperation when those communications are accessible inside the US.
- 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

---

* 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.

53358.105

Congress in both parties, and even in the civil liberties community, that a court order 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 (perhaps a very large percentage) of surveillance targeted at persons overseas will not affect the rights of people in the US. Furthermore, the NSA in most cases when it is targeting a person overseas cannot be sure in advance whether the particular targeted person overseas will sometime in the future have a communication with someone in the US. Therefore, it is reasonable to allow NSA to begin surveillance of targets overseas without a particularized order on the presumption that surveillance targeted at a person overseas will not interfere with the rights of Americans.

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.

---

[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.)

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 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.

-- The Analogy to Wiretaps in Criminal Investigations Shows That a Warrant Is Crucial

Law and practice governing more familiar wiretaps in criminal cases may help explain the situation here: If the government is wiretapping the phone of a Mafia don, it will inevitably intercept communications with a range of other persons, from the don's criminal associates to the pediatrician for his children. The government will listen to the communications with the pediatrician to determine who he is and whether he is involved in the don's criminal conduct.[2] If the police overhear the pediatrician discussing insurance fraud with the don, they can use that evidence against the doctor, even if they did not suspect at the outset of the surveillance that he was involved in criminal conduct. On the other hand, the doctor may be innocent, but the police may initially suspect he is in league with the don, and may share that information with the FBI, who may instigate a fruitless but damaging investigation of the doctor before they conclude he is innocent.

In this case, if the surveillance is court authorized, the doctor has no ground to complain about the monitoring of his calls, whether he is guilty or innocent. As has been noted, "a valid eavesdropping order of necessity permits the interception of communications of at least two parties." *People v. Gnozzo,* 31 N.Y.2d 134, 335 N.Y.S.2d 257, 265, 286 N.E.2d 706, 711 (1972). On the other hand, if the surveillance is not court authorized, the doctor has both constitutional and statutory grounds to complain. The fact that the government was targeting the don does not diminish the injury to the doctor – he has a claim for Fourth Amendment violation of his rights, and he has a civil claim under Title III for warrantless surveillance.

As in the criminal case, the presence or absence of a court order makes all the difference to the rights of the non-targeted person.

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.

---

[2] *See United States v. Ozar*, 50 F.3d 1440, 1448 (8th Cir. 1995), *cert. denied*, 116 S.Ct. 193 (1995) (upholding the "two minutes up/one minute down" technique recommended by the Justice Department, in which FBI agents listened to two out of every three minutes of every phone conversation).

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[3] and the PAA has a procedure for FISA court review of certain procedures, but it is woefully inadequate. The minimal judicial review in the PAA does not protect the rights of Americans and does not provide assurance of the Act's constitutionality:

- The PAA does not submit the right questions to judicial review. The PAA requires the Administration to submit to the FISA court procedures either for

[3] "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.

ensuring that the persons being targeted are outside the U.S. or for determining that the acquisitions conducted under 105B do not constitute electronic surveillance.[4] We have no doubt that the government will easily meet either or both requirements. The additional, and much more important, 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 persons or entities whose communications 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.

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: Blanket Orders to Target Persons Abroad

In short, it is unreasonable in a practical sense to require particularized orders when targeting persons overseas, but it is unreasonable in a constitutional sense to leave solely to unguided Executive Branch discretion surveillance activity in the US that will undeniably result in the interception of communications to and from Americans.

---

[4] There seems to be a drafting error in the PAA. The new Section 105B(a)(1) states that the court shall review pursuant to Section 105C procedures for determining that acquisitions of foreign intelligence under Section 105B concern persons reasonably believed to be outside the US, but Section 105C only requires the Attorney General to submit to the court and the court to assess procedures by which the government determines that acquisitions under Section 105B do not constitute electronic surveillance.

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 may leave 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

The Administration's one word answer to concerns about the effect of the PAA on the rights of Americans is "minimization." 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 if the NSA or another agency, in its sole discretion, decided to "target" the persons they were talking to overseas.

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 collecting 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]

It is apparent that the concept of minimization as applied by the NSA in recent years has permitted the retention and dissemination of considerable quantities of information about US persons. *Newsweek* reported in May 2006 that between January 2004 and May 2006, NSA had supplied the names of some *10,000* American citizens to various interested officials in other agencies.[5] It has also 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.[6] According to one report, under the NSA's new practice, the FBI was

---

[5] 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.

[6] Eric Lichtblau and Scott Shane, "Files Say Agency Initiated Growth of Spying Effort." *New*

flooded with information identifying U.S. persons.[7]

The terrorist watch list is a perfect example of how the wider dissemination of information 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.[8] 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.

The intelligence agencies are under Congressional and Presidential mandates to share information, including information about US persons. They are doing so, and they are relying on shared information, including erroneous information, to make decisions affecting people in their ordinary lives. Minimization is no longer being applied – and probably should not be applied – to block dissemination of information about US persons. There need to be other protections.

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

---

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 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.

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

[8] 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.

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.

The Administration complains that a "significant number" standard is unworkable, arguing that it often is not possible to tell whether a communication is with a US person. We believe that these questions can be resolved by the court, applying the Fourth Amendment and using the Administration's own processes for determining whether a communication involves a US person. Administration officials have assured the Congress that they are able to distinguish US person communications for purposes of applying the minimization rules.[9] While those minimization procedures no longer block dissemination of US person information, they do require an assessment be made as to whether information is about a US person. This same determination can be used as the basis for periodic reports to the FISA court. And the court can determine whether surveillance is affecting the Fourth Amendment 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.

---

[9] "[W]e have well established mechanisms for properly handling communications of U.S. persons that may be collected incidentally. These procedures, referred to as minimization procedures, have been used by the IC for decades. Our analytic workforce has been extensively trained on using minimization procedures to adequately protect U.S. person information from being inappropriately disseminated. ... These minimization procedures apply to the acquisition, retention and dissemination of U.S. person information. These procedures have proven over time to be both a reliable and practical method of ensuring the constitutional reasonableness of IC's collection activities. Testimony of DNI J. Michael McConnell before the House Permanent Select Committee on Intelligence, September 20, 2007 at p. 12.

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.

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.

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.

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 create vulnerabilities that can be exploited by hacker, other criminals, or foreign adversaries and could have other unintended negative consequences for privacy and security.[10]

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.

---

[10] 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.

IV. The Original FISA Required a Warrant for Some Communications To and From People in the US; The "Radio Exception" Is Not a Proxy for Excluding all Communications To and From the US

The Administration claims that the PAA restores FISA to its original purpose. It claims to find this purpose both in FISA's language and in the history of the development of global communications networks over the past 30 years. Upon examination, the Administration's claim appears to be made of whole cloth. It finds no support in the text of FISA, in its legislative history, or in the history of the development of telecommunications networks.

A. The Text of FISA Does Not Show An Intent to Exclude All Foreign-to-Domestic Calls Unless a Person in the US Was Being Targeted

When FISA was adopted, it did not apply to the interception in the US of radio signals (including satellite transmissions of telephone calls) unless all parties to the radio communication were in the US or the government was intentionally targeting a particular known US person located in the US. The Administration takes a very odd view of this treatment of radio communications, claiming that it was really an exception for all communications between Americans and people abroad:

> Congress designed a judicial review process that would apply primarily to surveillance activities within the United States where privacy interests are the most pronounced and not to overseas surveillance where privacy interests are minimal or non-existent. Congress gave effect to this careful balancing through its definition of the statutory term "electronic surveillance," the term that identifies those government activities that fall within the scope of the statute and, by implication, those that fall outside it. Congress established this dichotomy by defining "electronic surveillance" by reference to the manner of the communication under surveillance -- by distinguishing between "wire" communications -- which included most of the local and domestic traffic in 1978 -- and "radio" communications -- which included most of the transoceanic traffic in that era.
>
> Based on the communications reality of that time, that dichotomy more or less accomplished the Congressional purpose, as it distinguished between domestic communications that generally fell within FISA and foreign international communications that generally did not.[11]

This is a strange reading of FISA and is completely refuted by the fact that FISA in 1978 required warrants for interception of wire communications into and out of the US without regard to who was being targeted. If Congress had really wanted to exempt all calls to and from the US, it could easily have said so. As Mr. Wainstein's comments imply, and

[11] Prepared Remarks of Kenneth L. Wainstein, Assistant Attorney General for National Security, on FISA Modernization at the Georgetown University Law Center's National Security Center, September 10, 2007 http://www.usdoj.gov/opa/pr/2007/September/07_nsd_699.html.

as we explain below in a little more detail, in 1978 some domestic calls were carried in part by radio (satellite and microwave) and some international calls went on wire (undersea cable). It would be odd if Congress, after years of debate in the 1970s leading to the enactment of FISA, settled for a law that "more or less" accomplished its purpose by using a wire-radio distinction as a proxy for the much more direct international versus domestic distinction that the Administration wants to find to support the PAA.

B. In 1978, Some International Communications Were Carried By Wire, and Some Domestic Calls Were Carried by Radio

The Administration tries to bolster its argument that the "radio exception" was a proxy for an international communications to and from persons in the US by claiming that it matched the topography of international communications. DNI McConnell has argued:

> When the law was passed in 1978, almost all local calls were on a wire and almost all international communications were in the air, known as "wireless" communications. Therefore, FISA was written to distinguish between collection on a wire and collection out of the air.[12]

History does not bear this out: In 1978, many international calls were carried by wire and many domestic calls were carried in part by radio. A cursory review of the history of communications technology reveals that, in 1978, (1) both cable and satellite were being used for international communications into and out of US and (2) both cable and satellite were being used for domestic-to-domestic communications. In terms of relative volume, there was certainly an ebb and flow. Throughout the 1960s and 1970s, AT&T installed a network of transoceanic cables to carry telephone and other communications, and until 1965, essentially all telephone communications international and domestic were carried by wire. The first Intelsat satellite for international telephone went up in 1965, offering better speed and lower cost, but the industry continued to lay undersea cable. AT&T laid its 6th major undersea cable to Europe in 1976, when debate over FISA began in earnest, and it completed its 7th major trans-Altantic cable in 1978, the year FISA was adopted. Meanwhile, satellites were also being deployed and used for domestic-to-domestic calls: the first Comstat satellite for long-distance domestic calls went up in 1974. Satellites may have carried a majority of international calls in 1978, but they clearly did not carry all. The trend reversed itself again in 1988, when the first fiber optic cable was laid under the Atlantic, although satellites have improved too and continue to this day to carry a substantial amount of telephone traffic.

James Baker, former head of OIPR, summed up the history in his testimony last week to the House Intelligence Committee:

> With respect to the historical record, I've been looking at some documents

[12] Testimony of DNI J. Michael McConnell before the House Permanent Select Committee on Intelligence, September 20, 2007 at p. 5.

lately, just in a preliminary manner, that seem to indicate that trans-oceanic communications were made in relatively large quantities by both satellite and coaxial cables underneath the sea, that both kinds of systems were expected to continue in service for many years and, indeed, that the use of fiber optics was already anticipated for undersea cables.

C. Was the "Radio Exception" a Foreign-to-Foreign Exception?

There is one simple explanation for FISA's radio exception: The NSA's antennae in the US were used to intercept foreign-to-foreign communications. Further research may be useful. In 1978, did foreign-to-foreign communications transit the US via satellite connections into and out of US ground stations. It seems clear that NSA's facilities in the US have long had various capabilities to intercept radio signals to and from various points around the world. The diversity of these signals intelligence activities was too complex – and perhaps too sensitive -- for Congress to spell out in legislation. But by "exempting" radio, Congress may have been trying to make it clear that the interception on US soil of foreign-to-foreign communications did not require court order.

D. The Radio Exception Was Meant to Be Temporary, Not to Become the Rule for All Technologies

In the final analysis, arguments about the legislative intent of FISA must yield to considerations about what is right today to protect both the national security and the rights of Americans.

It is clear from FISA's legislative history that Congress intended to consider subsequent legislation to regulate interception of radio communications. The Senate Judiciary Committee's 1977 report on FISA, Rept 95-604, states:

> "The reason for excepting from the definition of 'electronic surveillance' the acquisition of international radio transmissions, including international wire communications when acquired by intercepting radio transmission when not accomplished by targeting a particular United States person in the United States, is to exempt from the provisions of the bill certain signals intelligence activities of the National Security Agency.
>
> Although it is desirable to develop legislative controls in this area, the Committee has concluded that these practices are sufficiently different from traditional electronic surveillance techniques, both conceptually and technologically, that, except when they target particular United States citizens or resident aliens in the United States, they should be considered separately by the Congress. ***The fact that this bill does not bring these activities within its purview, however, should not be viewed as congressional authorization of such activities.*** " P. 34 (emphasis added).

"The activities of the NSA pose particularly difficult conceptual and technical problems which are not dealt with in this legislation. Although many on the Committee are of the opinion that it is desirable to enact legislative safeguards for such activity, the committee adopts the view expressed by the Attorney General during the hearings that enacting statutory controls to regulate the NSA and the surveillance of Americans abroad raises problems best left to separate legislation. This language insures that certain electronic surveillance activities targeted against international communications for foreign intelligence purposes will not be prohibited absolutely ***during the interim period*** when the activities are not regulated by chapter 120 and charters for intelligence agencies and legislation regulating international electronic surveillance have not yet been developed." P. 64 (emphasis added).

V. In a Major Change, the PAA Appears to 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

The ambiguous language of the PAA presents several unanswered questions, notably –

- **Which agencies can exercise the new authority?** There seems to be no limit on the agencies to which Section 105B authority can be granted. In the past, E.O. 12333, which is being rewritten, has limited which agencies could perform electronic surveillance, but the PAA carves certain acquisitions of communications out of FISA's definition of electronic surveillance. It is impossible to predict what relationship the Administration will define between the PAA and the new E.O. on intelligence activities, but many agencies could

have the power to compel service provider cooperation with acquisition of communications.

- **What persons can orders be served upon?** Under Section 105B(e) of the PAA, the Director of National Intelligence and the Attorney General may direct *any person* to provide the government with assistance. Compare this with 50 U.S.C. 1802(a)(4). Under the PAA, the certification compelling cooperation need not be addressed to the service provider as an entity, but could be directed to an individual employee, suggesting that the acquisition of communications could occur without the knowledge or oversight of the senior management of the service provider.
- **What communications can be acquired?** It is clear that the PAA applies to real-time communications and it is pretty clear that it applies to stored email. What about the communications that occur daily as part of the global airline reservation system, which contain foreign intelligence concerning persons outside the US? What about Electronic Funds Transfers and other inter-bank communications? Every time a credit card is read at a point of sale, there is a communication between the point of sale and the credit card network, indicating essentially where the credit card holder is and what he is doing. Are these communications covered? Are the credit card companies providers of communications services to themselves and the merchants who accept the cards?

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.

United States Senate
Committee on the Judiciary

< Return To Hearing

Statement of

The Honorable Russ Feingold

United States Senator
Wisconsin
September 25, 2007

Statement for the Record of
Russell D. Feingold, United State Senator
Senate Judiciary Committee Hearing on
"Strengthening FISA: Does the Protect America Act Protect
Americans' Civil Liberties and Enhance Security?"
September 25, 2007

Mr. Chairman, this hearing is critically important. Before leaving town for the August recess, Congress rushed through legislation that grants too much unchecked authority to the executive branch and does not adequately protect the privacy of ordinary Americans. The administration successfully pushed the so-called "Protect America Act" through both houses in a matter of days without the deliberative process that this legislation needed. The result, predictably, was a bad bill that was quickly signed into law.

But that legislation expires early next year. I am pleased that the Senate Judiciary Committee is now taking a close look at this legislation as Congress considers whether and how to renew it. This committee's expertise in privacy and civil liberties, and in the Foreign Intelligence Surveillance Act (FISA), is very important to this debate.

This new law was billed as an effort to address a problem every member of Congress agreed should be fixed: making clear that when suspected terrorists are communicating, and both ends of the communication are on foreign soil, the U.S. government does not need a warrant to listen in.

Instead, the Protect America Act went much further. It dramatically broadens the government's authority to listen in on the conversations of anyone outside the United States without a warrant, even if that person is a U.S. citizen overseas, and even if he or she is talking to someone in the United States. As a result, the government has more power to monitor the conversations of American college students spending a semester abroad, servicemembers in Iraq and elsewhere, and journalists reporting from overseas, without their knowledge and without judicial oversight.

The new law also contains ambiguous language that could allow domestic spying without a warrant, permitting the government to conduct searches and obtain sensitive business records in certain circumstances without court review. Members of the administration have said that they do not intend to interpret the new law this broadly, even though they rejected a more reasonable alternative Democratic bill that would have fixed the foreign-to-foreign problem without including such broad language. But this is the same administration that claimed, in one of the more absurd legal arguments I have ever heard, that the authorization Congress passed to use military force in Afghanistan after 9/11 somehow allowed it to wiretap Americans in the United States without a warrant. And for years they did so in secret. So when members of the administration say, as they have in recent days, that we should trust them because they won't abuse this new law, members of Congress and the public have every right to be skeptical.

Now, instead of working with Congress to address the problems with this law, which expires in early 2008, the administration has launched an offensive to make the law permanent. Once again, it is attempting to turn what should be a serious, substantive debate into a political contest, using the tired tactics of exaggeration, intimidation, and fear-mongering.

This time, Congress needs to act responsibly and not be intimidated into giving the administration powers it does not need and could too easily abuse. We need to clarify the ambiguities in the law, and we need to fix several fundamental flaws: the lack of meaningful court involvement in overseeing the government's determination whether a target is overseas; the lack of privacy protections for Americans; and the lack of

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00190 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.123

adequate congressional or administrative oversight.

We must improve the process for determining whether the target of a wiretap is overseas by requiring the government to submit the methods by which it determines a target is overseas to the FISA Court in advance, and giving the Court a full opportunity to consider those methods.

Congress should also strengthen the privacy protections for Americans by requiring that the government obtain an individualized FISA Court warrant to wiretap a U.S. citizen overseas, and by involving the Court when the government conducts surveillance of communications between foreign targets and individuals in the United States. Technological advancement has led Americans to engage in more international communications than ever before, and we need to ensure that their privacy rights in these communications are protected.

Finally, Congress should toughen oversight of the process by creating regular, meaningful congressional reporting requirements on these new authorities, as well as provisions for oversight by the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, and the National Security Agency.

Congress should never have passed the Protect America Act, even for six months. Instead of blindly approving this expansive authority yet again, Congress should fix this law to make sure we protect Americans' privacy as we wiretap terrorists and other foreign intelligence targets. Let's get it right this time.

Thank you, Mr. Chairman.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00191 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.124

United States Senator Chuck Grassley
Iowa
http://grassley.senate.gov

Prepared Statement of Senator Chuck Grassley of Iowa
U.S. Senate Committee on the Judiciary
"Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?"
Tuesday, September 25, 2007

Mr. Chairman, thank you for holding this hearing today to examine the Protect America Act passed by Congress prior to the August recess. I believe that this hearing is necessary to address important questions surrounding the collection and review of intelligence gathered in accordance with the Protect America Act and the original Foreign Intelligence Surveillance Act (FISA) passed in 1978. This is a very sensitive area and given that we are in an open, unclassified setting we must be mindful of the questions we ask. That said, Congress must continue its important work to fulfill its Constitutional duty and conduct oversight over both the collection and gathering of intelligence to ensure that the rights of U.S. citizens are upheld.

I appreciate Director of National Intelligence McConnell's testimony and thank him for making himself available to the Committee and to members to discuss the Protect America Act and necessary updates to FISA. Further, I'd also like to thank the countless individuals in our intelligence community who have worked diligently in protecting our country and our soldiers by providing vital intelligence and information.

Since the attacks on September 11, 2001, this Committee has reviewed FISA and the process surrounding the collection of foreign intelligence numerous times. Immediately following September 11, Senator Leahy, Senator Specter and I conducted a review of the activities of the FBI and the Department of Justice in utilizing FISA to collect evidence against Zacarias Moussaoui. In February of 2003, we issued an interim report on FISA Implementation Failures by the FBI. This report concluded that FBI officials misapplied FISA requirements regarding the determination of whether Moussaoui was an agent of a foreign power under the FISA statute. Further, our report found that the FBI failed in applying the applicable standard for determining when probable cause existed under the FISA statute. Finally, and most notably, the report found that "FBI personnel involved in the FISA process were not properly trained to carry out their important duties." These failures were real and raised serious questions about the handling of national security matters by the Department of Justice and the FBI.

The 2003 report is a reminder of this Committee's mission in conducting oversight over the Department of Justice and the FBI. We must be cognizant that both DOJ and FBI play a vital role in interpreting and applying the letter of the FISA statute. At the

53358.125

same time, must also be sure that adequate training, education, and resources are devoted to the Department of Justice and the FBI as they work to implement any changes we make to FISA.

Mr. Chairman, we have a duty to the American people to ensure that as we address the Protect America Act and the FISA statute as a whole, that we pass a law that is not only understandable to the intelligence community, but one that is workable for law enforcement as well.

Although I will be unable to attend the hearing as I must serve as the Ranking Member at a hearing before the Committee on Finance, I thank the Chairman for holding this hearing and look forward to the testimony of the witnesses.

-30-

53358.126

United States Senate
Committee on the Judiciary

< Return To Hearing

Statement of

The Honorable Patrick Leahy

United States Senator
Vermont
September 25, 2007

STATEMENT OF SEN. PATRICK LEAHY,
CHAIRMAN, SENATE JUDICIARY COMMITTEE
HEARING ON "STRENGTHENING FISA: DOES THE PROTECT AMERICA ACT PROTECT AMERICANS' CIVIL LIBERTIES AND ENHANCE SECURITY?"
SEPTEMBER 25, 2007

The Committee holds this hearing today to consider the Protect America Act, passed in haste in early August.

Congressional leaders went to extraordinary lengths earlier this summer to provide the flexibility Director McConnell said was needed to fix a legal problem with surveillance of targets overseas. I supported a change to FISA, as I have done several times since 9/11. The Rockefeller-Levin legislative proposal that many of us voted for would have eliminated the need to get individual probable cause determinations for surveillance of overseas targets. That bill addressed the concern that had been raised by an opinion of the FISA Court, and it satisfied what the Administration said was needed in that time of heightened concern. Yet, Director McConnell and the Administration rejected that legislation. We need to find out why.

I do not know who Director McConnell is referring to in his written testimony when he says that he has "heard a number of individuals . . . assert that there really was no substantial threat to our nation." I trust that he is not referring to any Senator serving on this Committee. Let me be clear: Every single Senator understands the grave threats to our Nation. Every Senator wants us to be able to conduct surveillance effectively. Every Senator on this Committee voted to give him the flexibility he said he needed. I hope we will not hear anymore irresponsible rhetoric about congressional inquiries risking Americans' safety. We all want Americans to be safe. Our job is to protect Americans' security and Americans' rights.

The Protect American Act provides sweeping new powers to the Government to engage in surveillance, without a warrant, of international calls to and from the United States and potentially much more. It does this, in the view of many, without providing any meaningful check or protection for the privacy and civil liberties of the Americans who are on those calls. We are asked to trust that the Government will not misuse its authority. When the issue is giving muscular new powers to government, "just trust us" is not enough.

Fortunately, those temporary provisions contain a sunset. We meet today to consider real issues and concerns with this legislation. Let us not engage in the high-pitched rhetoric that plays on people's fears and prevents real progress.

The FISA Court has played an important role ever since the Foreign Intelligence Surveillance Act was passed to provide a meaningful check on the actions of our Government as it engaged in surveillance of Americans. Unfortunately, the FISA Court was cut out of any meaningful role in overseeing surveillance of Americans in the Protect America Act.
The Rockefeller-Levin measure by contrast would have allowed the "basket" surveillance orders that the Administration says are needed, with no individual probable cause determinations, but it had the FISA Court issuing those orders to communications carriers after reviewing the Administration's procedures. The Protect America Act requires U.S. telecommunications carriers to assist with surveillance just on the say-so of the

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00194 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.127

Attorney General and the Director of National Intelligence. That is a mistake; it is an invitation to abuse.

I look forward to hearing from Director McConnell on what he believes the problems are with a role for the FISA Court in issuing orders, and how we can create the necessary authority to include the appropriate checks and balances.

The problem facing our intelligence agencies is targeting communications overseas. We want them to be able to intercept calls between two people overseas with a minimum of difficulty. What changes the equation and raises the stakes is that the people may be innocent Americans, or they may be talking to innocent people here in the United States. International communications include those of businesspeople, tourists, and even the families of our troops overseas. We can give the Government flexibility it needs to conduct surveillance of foreign targets, while doing a better job protecting the privacy of innocent Americans.

The Protect America Act provides no meaningful check by the FISA Court or the Congress. It does not even require the Government to have its own internal procedures for protecting the privacy of these Americans. The alternative bill would have required internal procedures and an Inspector General audit. I would like to know why Director McConnell rejected that check.

In addition, the Protect America Act contains language that appears to go far beyond what the Administration said it needed. It redefines "electronic surveillance" in a way that has expansive implications, but was not necessary to accomplish the Administration's stated objectives. It has language in many places that, at the very least, is inscrutable and could be read to allow much broader surveillance than the Administration has acknowledged or, I hope, intends. If this was unintentional, let us fix it. If it was not, then we need to evaluate what was really intended and why.

I know the skilled and dedicated employees of our intelligence agencies want to protect our country. But if our history has taught us anything, it is that the Government can not and should not be left to police itself when it comes to the secret surveillance of Americans. The Founders knew it. The Congress that passed the Foreign Intelligence Surveillance Act knew it. I hope this hearing will help us institute the proper protections to safeguard our security and our valued freedoms.

# # # # #

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00195 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.128

UNCLASSIFIED
9-21-07

Senate Committee on the Judiciary

Hearing on the
Foreign Intelligence Surveillance Act
and
Implementation of the Protect America Act

25 September 2007

Statement for the Record

of

J. Michael McConnell

UNCLASSIFIED

53358.129

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

BEFORE THE
JUDICIARY COMMITTEE
UNITED STATES SENATE

September 25, 2007

Good morning Chairman Leahy, Ranking Member Specter, and Members of the Committee:

Thank you for inviting me to appear here today in my capacity as head of the United States Intelligence Community (IC). I appreciate this opportunity to discuss the 2007 Protect America Act; updating the Foreign Intelligence Surveillance Act; and our implementation of this important new authority that allows us to more effectively collect timely foreign intelligence information. I look forward to discussing the need for lasting modernization of the Foreign Intelligence Surveillance Act (FISA), including providing liability protection for the private sector.

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

I have not appeared before this Committee previously as a witness, and so I would like to take a moment to introduce myself to you. I am a career intelligence professional. I spent the majority of my career as a Naval Intelligence Officer. During the periods of Desert Shield and Desert Storm, as well as during the dissolution of the Soviet Union, I served as the primary Intelligence Officer for the Chairman of the Joint Chiefs of Staff and the Secretary of Defense. I then had the privilege of serving as the Director of

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00197 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.130

the National Security Agency (NSA) from 1992 to 1996, under President Clinton. In 1996, I retired from the U.S. Navy after 29 years of service - 26 of those years spent as a career Intelligence Officer. I then turned to the private sector as a consultant, where for ten years I worked to help the government achieve better results on a number of matters, including those concerning intelligence and national security. I have been in my current capacity as the nation's second Director of National Intelligence (DNI) since February 2007.

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

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

Also, over a year ago, Members of Congress were concerned about FISA, and how its outdated nature had begun to erode our intelligence collection capability. Accordingly, since 2006, Members of Congress on both sides of the aisle have proposed legislation to modernize FISA. The House passed a bill last year. And so, while the Protect America Act is new, the dialogue among Members of both parties, as well as between the Executive and Legislative branches, has been ongoing for some time. In my

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00198 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.131

experience, this has been a constructive dialogue, and I hope that this exchange continues in furtherance of serving the nation well.

The Balance Achieved By FISA

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

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

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

FISA has a number of substantial requirements, several of which I will highlight here. A detailed application must be made by an Intelligence Community agency, such as the Federal Bureau of Investigation (FBI), through the Department of Justice, to the FISA Court. The application must

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00199 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.132

be approved by the Attorney General, and certified by another high ranking national security official, such as the FBI Director. The applications that are prepared for presentation to the FISA Court contain extensive information. For example, an application that targets an agent of an international terrorist group might include detailed facts describing the target of the surveillance, the target's activities, the terrorist network in which the target is believed to be acting on behalf of, and investigative results or other intelligence information that would be relevant to the Court's findings. These applications are carefully prepared, subject to multiple layers of review for legal and factual sufficiency, and often resemble finished intelligence products.

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

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

Technology Changed

Why did we need the changes that the Congress passed in August? FISA's definition of electronic surveillance, prior to the Protect America Act and as passed in 1978, has not kept pace with technology. Let me explain what I mean by that. FISA was enacted before cell phones, before e-mail, and before the Internet was a tool used by hundreds of millions of people

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00200 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.133

worldwide every day. When the law was passed in 1978, almost all local calls were on a wire and almost all international communications were in the air, known as "wireless" communications. Therefore, FISA was written to distinguish between collection on a wire and collection out of the air.

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

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

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

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

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

For these reasons, prior to Congress passing the Protect America Act last month, in a significant number of cases, IC agencies were required to make a showing of probable cause in order to target for surveillance the communications of a foreign intelligence target located overseas. Then, they needed to explain that probable cause finding in documentation, and obtain approval of the FISA Court to collect against a foreign terrorist located in a

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00201 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.134

foreign country. Frequently, although not always, that person's communications were with another foreign person located overseas. In such cases, prior to the Protect America Act, FISA's requirement to obtain a court order, based on a showing of probable cause, slowed, and in some cases prevented altogether, the Government's ability to collect foreign intelligence information, without serving any substantial privacy or civil liberties interests.

National Security Threats

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

Allow me to dispel that notion.

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

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

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

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

- Al-Qa'ida is and will remain the most serious terrorist threat to the Homeland, as its central leadership continues to plan high-impact

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00202 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.135

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

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

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

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

- We assess Lebanese Hizballah, which has conducted anti-U.S. attacks outside the United States in the past, may be more likely to consider attacking the Homeland over the next three years if it perceives the United States as posing a direct threat to the group or Iran.

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

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00203 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.136

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

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

What Does the Protect America Act Do?

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

First, it clarified that the definition of electronic surveillance under FISA should not be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States. This provision is at the heart of this legislation: its effect is that the IC must no longer obtain court approval when the target of the acquisition is a foreign intelligence target located outside the United States.

This change was critical, because prior to the Protect America Act, we were devoting substantial expert resources towards preparing applications that needed FISA Court approval. This was an intolerable situation, as

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00204 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.137

substantive experts, particularly IC subject matter and language experts, were diverted from the job of analyzing collection results and finding new leads, to writing justifications that would demonstrate their targeting selections would satisfy the statute. Moreover, adding more resources would not solve the fundamental problem: this process had little to do with protecting the privacy and civil liberties of Americans. These were foreign intelligence targets, located in foreign countries. And so, with the Protect America Act, we are able to return the balance struck by Congress in 1978.

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

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

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

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

By passing this law, Congress gave the IC the ability to close critical intelligence gaps. When I talk about a gap, what I mean is foreign intelligence information that we should have been collecting, that we were not collecting. We were not collecting this important foreign intelligence information because, due solely to changes in technology, FISA would have required that we obtain court orders to conduct electronic surveillance of foreign intelligence targets located outside the United States. This is not what Congress originally intended. These items:

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00205 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.138

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

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

Common Misperceptions About the Protect America Act

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

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

The motivation behind the Protect America Act was to enable the Intelligence Community to collect foreign intelligence information when targeting persons reasonably believed to be outside the United States in order to protect the nation and our citizens from harm. Based on my discussions with many Members of Congress, I believe that there is substantial, bipartisan support for this principle. There are, however,

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00206 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.139

differences of opinion about how best to achieve this goal. Based on the experience of the Intelligence Community agencies that do this work every day, I have found that some of the alternative proposals would not be viable.

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

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

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

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

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00207 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.140

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

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

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

Moreover, for operational reasons, the Intelligence Community has little incentive to engage in reverse targeting. If a foreign intelligence target who poses a threat is located within the United States, then we would want to investigate that person more fully. In this case, reverse targeting would be an ineffective technique for protecting against the activities of a foreign intelligence target located inside the United States. In order to conduct electronic surveillance or physical search operations against a person in the United States, the FBI, which would conduct the investigation, would seek FISA Court approval for techniques that, in a law enforcement context, would require a warrant.

Oversight of the Protect America Act

Executive Branch Oversight

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00208 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.141

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

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

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

FISA Court Oversight

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

> (a) No later than 120 days after the effective date of this Act, the Attorney General shall submit to the Court established under section

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00209 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.142

> 103(a), the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance. The procedures submitted pursuant to this section shall be updated and submitted to the Court on an annual basis.

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

Congressional Oversight

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

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

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

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00210 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.143

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

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

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

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

On September 12, 2007, at the request of the professional staff of the Senate Intelligence Committee, the Assistant Attorney General of the National Security Division, and the General Counsels of the ODNI, NSA, and FBI briefed staff members from the House Intelligence Committee, and the Senate Intelligence, Armed Services Committees, and this Committee regarding the implementation of the Protect America Act. In all, over twenty Executive Branch officials involved in Protect America Act implementation supported this briefing.

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

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00211 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.144

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

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

On September 17, 2007, representatives from the ODNI and the Department of Justice provided briefings regarding implementation to staff members from the House Judiciary Committee.

On September 18, 2007, Assistant Attorney General Ken Wainstein of the Department of Justice's National Security Division, my General Counsel, Ben Powell, and I testified before the Judiciary Committee of the House of Representatives on the Protect America Act.

On September 19, 2007, representatives from the ODNI and the Department of Justice provided briefings regarding implementation to staff members from this Committee.

On September 20, 2007, Assistant Attorney General Ken Wainstein of the Department of Justice's National Security Division and I testified before the House Permanent Select Committee on Intelligence in regard to the Protect America Act.

Also on September 20, 2007, I was joined by National Security Agency Director (NSA), Lieutenant General Keith Alexander; Assistant Attorney General Ken Wainstein of the Department of Justice's National Security Division; Acting Assistant Attorney General from the Department of Justice's Office of Legal policy, Brett Gerry; Federal Bureau of Investigation (FBI) Deputy Director John Pistole and the General Counsels of the ODNI, FBI, and NSA to speak to a closed session of the Select Committee on Intelligence of the Senate on the Protect America Act.

Additional Member and staff briefings shall follow.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00212 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.145

Lasting FISA Modernization

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

Making the Changes Made by the Protect America Act Permanent

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

Liability Protection

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

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

Streamlining the FISA Process

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00213 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.146

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

We also ask Congress to consider extending FISA's emergency authorization time period, during which the government may initiate surveillance or search before obtaining Court approval. We propose that the emergency provision of FISA be extended from 72 hours to one week. This change will ensure that the Executive Branch has sufficient time in an emergency situation to prepare an application, obtain the required approvals of senior officials, apply for a Court order, and satisfy the court that the application should be granted. I note that this extension, if granted, would not change the substantive findings required before emergency authorization may be obtained. In all circumstances, prior to the Attorney General authorizing emergency electronic surveillance or physical search pursuant to FISA, the Attorney General must make a finding that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. Extending the time periods to prepare applications after this authorization would not affect the findings the Attorney General is currently required to make.

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

Mr. Chairman, this concludes my remarks.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00214 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.147

Hearing of the

United States Senate

Committee on the Judiciary

Strengthening FISA:

Does the Protect America Act

Protect Americans' Civil Liberties and Enhance Security?

Tuesday, September 25, 2007

Testimony of Suzanne E. Spaulding

53358.148

Hearing of the

United States Senate

Committee on the Judiciary

Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?

Tuesday, September 25, 2007

Testimony of Suzanne E. Spaulding

Chairman Leahy, Ranking Member Specter, Members of the Committee, thank you for this opportunity to testify on changes to the Foreign Intelligence Surveillance Act (FISA). In the twenty years that I spent working on efforts to combat terrorism, at the Central Intelligence Agency, at both the House and Senate intelligence oversight committees, and as Executive Director of two different commissions, on terrorism and weapons of mass destruction, I developed a strong sense of the seriousness of the national security challenges that we face and deep respect for the men and women in our national security agencies who work so hard to keep our nation safe.

We owe it to those professionals to ensure that they have the tools they need to do their job; tools that reflect the ways in which advances in technology have changed both the nature of the threat and our capacity to meet it. Equally important, they deserve to have clear guidance on just what it is that we want them to do on our behalf -- and how we want them to do it. Clear rules and careful oversight provide essential protections for those on the front lines of our national security efforts. Unfortunately, the newly enacted changes to the Foreign Intelligence

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00216 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.149

Surveillance Act (FISA) provide neither clear guidance nor the mechanisms to ensure careful oversight.

Problems with the Protect America Act of 2007

Changing the Definition of Electronic Surveillance.

First, I would urge Congress to avoid trying to accomplish objectives by changing definitions. The terms in FISA not only appear throughout this complex statute; they are also referenced in or inform other laws, Executive Orders, directives, policies, etc. The risk of unintended consequences is significant, particularly when changing the definition of something a fundamental as electronic surveillance. The report recently prepared by the Congressional Research Service points out several ways in which defining a range of activity out of electronic surveillance (section 105A), while still setting up a potential process to authorize those activities within this statute designed to regulate electronic surveillance (section 105B), creates confusion. This does not even address the consequences for internal NSA directives and other legal and policy documents that reference electronic surveillance.

Most importantly, as Ken Wainstein noted in his testimony before the House Judiciary Committee on September 18, 2007, the definition of the statutory term electronic surveillance "is sort of the gatekeeper term in the statute that identifies those government activities that fall within the scope of the statute and, by implication, those that fall outside the scope of the statute." By defining out of FISA the acquisition of any communication when it is directed at someone reasonably believed to be outside the United States, you remove any statutory protection that FISA might otherwise provide for Americans whose communications might fall into this category.

None of the FISA provisions apply to intercepts defined out of FISA by section 105A. There is no statutory minimization requirement, no court review of any procedures before or after the fact, no reporting requirements. These intercepts are not covered by FISA at all. There may be Executive Orders, directives, or other internal policies that call for minimization of even these intercepts, but those can be changed unilaterally at any time by the Executive Branch.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00217 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.150

What about the requirements and safeguards in 105B? This section is an *optional* process that the Attorney General and the DNI "may" use if they require the assistance of a third party and need to compel that assistance. Some telecommunication providers, for example, may demand some sort of express legal authorization before they will help the government access communications inside the United States. In fact, prior to the talk of granting full retroactive immunity to carriers who helped with surveillance outside of FISA, I would have thought all telecom providers would have insisted on written assurances about the legal authority under which the government would be accessing their customers' communications. However, if companies can expect the government to protect them regardless, they may be more willing to help without regard to the law—in which case the government would not need to use the optional procedures and safeguards in 105B.

Notwithstanding Any Other Law.

Second, avoid using the words "notwithstanding any other law." This is how the new section 105B begins and these words should always raise a red flag. In this case, it raises serious questions about the continuing applicability of other laws that regulate the collection of intelligence inside the United States, including restrictions within FISA with regard to physical searches. If there are particular provisions of law that Congress wishes to ensure do not hamper the collection of this intelligence inside the US, they should specify those provisions and be clear about how they will and will not apply.

Section 105B provides authority for the AG and DNI to collect intelligence information inside the United States so long as (1) the information is about a person who happens to be outside the US at the time--including, of course, a US citizen, (2) the collection of that information does not involve electronic surveillance, and (3) the government requires the assistance of someone with access to a communication or communication equipment. It appears to be about electronic surveillance targeting someone outside the US (which is now no long considered "electronic surveillance"), but it in fact provides authorization for the government to gather any kind of communication and to gather it inside the United States. Thus, it would appear to authorize intercepting US mail between two people inside the United States, so long as the government reasonably believes the letter discusses, at least in part, someone outside the US.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00218 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.151

The careful legal regime governing mail intercepts is overruled by the "notwithstanding any other law" language" in section 105B.

Moreover, it would appear that the AG could authorize the physical search of your home to find a letter from your son overseas or the family computer on which you've stored his emails, although this would raise significant 4th Amendment issues. The FISA provisions that regulate physical searches become irrelevant because section 105B applies "notwithstanding any other law."

Similarly, the protections that Congress worked so hard to enact last year for section 215, the so-called business records provision, would also appear to be overruled under circumstances in which Section 105B applies. Thus, any individual who can help the government obtain access to communications that involve someone outside the United States can now be compelled to provide that assistance under section 105B, with fewer safeguards.

And it is not just other sections of FISA that are effectively repealed by this language. It appears to overrule any laws that might otherwise affect the gathering of information about communications that concern people outside the US. Thus, whatever privacy protections Congress may have enacted in other laws, including the Electronic Communications Privacy Act, would no longer have any impact on this activity.

The Administration has indicated that it did not intend for the law to have such broad implications and is willing to work with Congress to clarify the statutory language. I urge Congress to take them up on this offer and ensure that the law is narrowly drafted to fix only specific problems clearly identified and justified by the intelligence community.

Not Limited to Terrorism.

Despite this new law having been explained to the American public as necessary to protect them from the next terrorist attack, none of the intelligence collection it authorizes has to be related in any way to terrorism. It applies to any "foreign intelligence," a term which has been amended over the years to include a very broad range of information.

Inadequate Minimization.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00219 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.152

It is true that information gathered under 105B must be subjected to minimization procedures, but it appears that the statutory requirements that apply are the less rigorous procedures that apply when a FISA judge has reviewed a full FISA application and found probable cause to believe that the target of the surveillance was a foreign power or agent of a foreign power.

The Protect Act simply refers to "the minimization procedures in section 101(h)." There are two sets of minimization procedures proscribed in that section. The first set applies when a FISA judge has approved an application. The second set is much more stringent and applies when the Attorney General has approved surveillance without going to a FISA judge. These more rigorous procedures are statutorily limited to situations in which the AG is acting pursuant to the authority granted him in section 102(a). Thus, they would not apply to the unilateral authority granted to the AG and DNI in the Protect Act.

The general minimization procedures in 101(h)(1)-(3) reflect a recognition that, even after all the application requirements had been met and approved by a FISA judge, there remains some risk that information about U.S. persons (USPs) might be collected. These procedures require steps be taken to minimize the acquisition and retention, and prohibit the dissemination, of such information. However, the procedures are to be "reasonably designed in light of the purpose and technique" of the surveillance and "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." This is a very broad and flexible standard, particularly given the current scope of "foreign intelligence."

Under section 101(h)(4), if surveillance is conducted pursuant to AG authorization rather than a warrant from a FISA judge—a situation more analogous to the 105B authority-- no contents of any communication to which a USP is a party can be disclosed, disseminated, or used for any purpose or retained for more than 72 hours without getting a court order, unless the AG determines that the information indicates a threat of death or serious bodily harm. Concern about ensuring that electronic surveillance authorized unilaterally by the AG could not be used to gather information about USPs was so strong when FISA was enacted that even the mere

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00220 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.153

existence of such a communication was included in this restriction. At a minimum, this stricter procedure should apply to information collected under section 105B.

Require Proactive Efforts to Identify Parties' Locations.

The Protect Act requires that the AG and DNI develop procedures to reasonably ensure that the target is outside the US (or the information concerns someone outside the US and is not "electronic surveillance") but the Act does not provide any other requirements for those procedures.

The government should have a proactive obligation to take whatever steps are feasible, on an ongoing basis rather than just at the outset of surveillance or other intelligence collection, to determine whether the target is in fact overseas and whether the other party to a communication is inside the United States. The phone company always seems to be able to determine whether I am using my cell phone at home or overseas--I know this because they charge me a lot more when I use it overseas! There ought to be a way for the government to know, even if it is after the fact, where the parties to many of these communications are located. This begins to provide the basis for a legal regime that is much more narrowly focused, with precise procedures and safeguards to govern surveillance that involves persons inside the United States.

Ensure Independent Oversight.

Rigorous oversight of the use of this authority will be essential. The Administration has promised that it will provide such oversight and provide reporting to Congress, which is important and reassuring. However, given the reported failure of the Attorney General to properly report to Congress regarding problems with the use of national security letters, I would urge Congress to direct, in statute, that the Justice Department and DNI Inspectors General report jointly on implementation within 90 days of enactment and every 90 days thereafter.

Context for FISA Changes

The Administration has indicated that it plans to seek broader changes to FISA. As the committee and the Congress consider how to move forward on this issue, I would offer some

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00221 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.154

overarching thoughts on the challenge presented by the national security imperative to monitor communications of those who wish to do us harm.

First, any expansion of authority should be limited to terrorism targets. This is how the authority is sold to the American public by the Administration. To then broaden the authority to include any and all foreign intelligence on any topic is a kind of "bait and switch."

Second, craft the narrowest changes possible to remove whatever impediment has arisen to using FISA. Technology experts and FISA judges, current and former, can provide essential insights into what the government and the communications providers can and cannot do, as well as what safeguards are most important to prevent abuse.

Third, be extremely cautious about limiting the role of the FISA judges. As Supreme Court Justice Powell wrote for the majority in the *Keith* case, "The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. ...But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."

Finally, Congress should seek a stronger commitment from the Administration that it will actually abide by the law. As noted earlier, the new procedures under section 105B are optional; the AG and DNI "may" choose to use them but they are not required to follow this process. However, the rest of FISA is not optional. Until Congress gets some assurance from the Executive Branch about where they draw the line on Presidential authority in this area, it is hard to see why Members should continue to work so hard to craft careful laws.

On a related point, the Administration has indicated that it will be back in front of Congress seeking immunity for carriers and others who cooperated in the Terrorist Surveillance Program and, perhaps, other intelligence activities. It is hard to imagine a more powerful way to undermine respect for the rule of law and the critical role that communication providers play as

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00222 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.155

the last line of defense against government abuse. Moreover, it's not clear why this is needed. Under current law, communication providers already can avoid liability if they simply have a letter from the AG saying the government's request is legal. If they did not even get that, what message do we send by giving them immunity for totally disregarding the law? Why wouldn't the next telecommunications CEO decide to go ahead and ignore the legal requirements, figuring the government would bail the company out if it ever became public?

In an area such as this, where the normal safeguards of transparency are lacking, requiring communication providers to at least get a certification that the request to hand over customer information or allow communication intercepts is legal serves as an important potential deterrent to abusive behavior by the government. At a minimum, Congress needs to fully understand what past activities would be immunized before adopting such a wide-ranging provision.

Undertake a Broader Review of Domestic Intelligence Collection

FISA is the primary statute governing domestic intelligence collection. Rather than attempt to guess at what might really be needed to meet today's challenges and how these and other changes will affect our ability to meet those challenges and protect Americans' privacy, Congress should take the time to ensure they understand the full context in which these changes are being sought. This includes the problems that have prompted them, particularly as these relate to current and past intelligence activities and the changing nature of the threat, as well as how these new authorities, definitions, and procedures would relate to all of the other national security and law enforcement tools available to the government.

I urge Congress not to consider any "overhaul" of FISA without first undertaking a comprehensive review of domestic intelligence collection. The attacks of 9/11 revealed a vulnerability at home that led to a dramatic increase in domestic intelligence activity. The Federal Bureau of Investigation's priorities turned 180 degrees, as it was pressed to place domestic intelligence collection at the forefront rather than criminal law enforcement. But the FBI is not the only entity engaged in domestic intelligence. The Central Intelligence Agency, National Security Agency, Department of Defense, Department of Homeland Security, and state

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00223 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.156

and local law enforcement are among the many entities gathering intelligence inside the US. The threat to the homeland presents unique challenges, both to effective intelligence and to appropriate protections against unwarranted government intrusion.

Unfortunately, the legal framework governing this intelligence activity has come to resemble a Rube Goldberg contraption rather than the coherent foundation we expect and need from our laws. The rules that govern domestic intelligence collection are scattered throughout the US Code and a multitude of internal agency policies, guidelines, and directives, developed piecemeal over time, often adopted quickly in response to scandal or crisis and sometimes in secret.

Rather than continuing this pattern, the House of Representatives should consider establishing a Joint Inquiry or Task Force with representation from the most relevant committees (Intelligence, Judiciary, Armed Services, Foreign Affairs, and Homeland Security), to carefully examine the nature of the threat inside the US and the most effective strategies for countering it. Then this task force, the entire Congress, and the American public, can consider whether we have the appropriate institutional and legal framework for ensuring that we have the intelligence necessary to implement those strategies, with adequate safeguards and oversight.

The various authorities for gathering information inside the United States, including the authorities in FISA, need to be considered and understood in relation to each other, not in isolation. For example, as discussed earlier, Congress needs to understand how broader FISA authority relates to the various current authorities for obtaining or reviewing records, such as national security letters, section 215 of FISA, and the physical search pen register/trap and trace authorities in FISA, and the counterparts to these in the criminal context, as well as other law enforcement tools such as grand juries and material witness statutes.

Executive Order 12333, echoed in FISA, calls for using the "least intrusive collection techniques feasible." The appropriateness of using electronic surveillance or other intrusive techniques to gather the communications of Americans should be considered in light of other, less intrusive techniques that might be available to establish, for example, whether a phone number belongs to a suspected terrorist or the pizza delivery shop. It's not the "all or nothing" proposition often portrayed in some of the debates.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00224 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.157

Congress should undertake this comprehensive consideration of domestic intelligence with an eye toward the future but informed by the past and present. Until Congress fully understands precisely what has and is being done in terms of the collection and exploitation of intelligence related to activities inside the US, by all national security agencies, it cannot wisely anticipate the needs and potential problems going forward.

This applies particularly to changes to FISA. Congress must be certain that it has been fully informed about the details of the Terrorist Surveillance Program and any other surveillance programs or activities initiated after 9/11, not just in their current form but in the very earliest stages, including the legal justifications offered at the time the activities were initiated. Understanding how the law operates in times of crisis and stress is key to understanding how it might need to be strengthened or adjusted to meet national security imperatives in ways that will protect against future abuse.

Conducting this kind of careful and thorough oversight is particularly challenging in today's environment, as we saw with the rush to enact the Protect Act just before the August recess. Congress' ability to insist that the expansion of authority be appropriately limited and safeguarded was significantly hampered by concerns that the American public would view Members as "soft" on national security.

Reshape discussions about how best to address the terrorist threat

Effective oversight and thoughtful legislation will require reshaping the discussion about how to best address the long term threat of terrorism. We need a broader discussion about the ways in which policies that mock the rule of law and undermine our carefully constructed system of checks and balances make it more likely, rather than less likely, that we will be attacked again.

Military and civilian experts agree that the long-term threat from international terrorism is not going to be defeated militarily. In addition to eliminating the terrorists' leadership, it is at least equally essential to reduce their ability to recruit new young people to join their "cause" and to generate and maintain support within communities around the world. This is a struggle for hearts and minds; a competition of narratives. The "jihadist" narrative is undeniably compelling

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00225 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.158

to many young Muslim men—and we unfortunately strengthen this narrative when we speak in terms of a Global War on Terrorism. The narrative of democracy, individual freedoms, and the rule of law can be equally compelling but its credibility is dramatically undermined if the greatest democracy is not clearly committed to living that narrative rather than simply mouthing the words.

We have to demonstrate that we still believe what our founders understood; that this system of checks and balances and respect for civil liberties is not a luxury of peace and tranquility but was created in a time of great peril as the best hope for keeping this nation strong and resilient. It was a system developed not by fuzzy-headed idealists but by individuals who had just fought a war and who knew that they faced an uncertain and dangerous time. They saw first-hand the how the whims of a single, unchecked ruler could lead a country astray. They knew that in times of fear and crisis, the instinct is to reach for power--and they determined that balancing power between all three branches would protect against that frailty of human nature and ultimately make for wiser, better decisions and a more unified and strong nation.

Our greatest weapon against global terrorism is a committed and determined American public. Public support is strengthened by developing consensus through public discussion and debate-not by developing policies in secret or by stifling dissent by labeling those who disagree as "unpatriotic" or insufficiently aware of the post 9/11 threat. Statements claiming that Congressional debate over proposed FISA changes costs American lives are not only suspect in terms of credibility, they also reflect a fundamental failure to appreciate the strength of our democracy.

The wisdom of this system and the importance of remaining true to it even in times of peril can perhaps best be understood with regard to fears of home-grown terrorism. The best hope for detecting and preventing this threat lies not in intrusive intelligence methods, which are better suited to monitoring a known target than in finding out who might be a target. Instead, our best hope lies in working closely with communities, particularly Muslim American communities. Yet, many of our policies and practices since 9/11 that unnecessarily compromise civil liberties

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00226 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.159

or seem to reflect a lack of respect for the rule of law risk alienating those very communities. In this regard, they make us less secure.

It is also clear that the failure of the Administration to follow the law or take advantage of our system of checks and balances in its implementation of the Terrorist Surveillance Program, and other related intelligence activities, had significant negative consequences for our national security. The Administration tells us that these surveillance activities were, and are, vital to our security. Yet here are some of the consequences of the failure to build a firm legal foundation for these programs:

* ***The program was shut down for weeks:*** The shaky legal ground for surveillance activities apparently caused sufficient concern by the Acting Attorney General and the FBI Director that the program was reportedly shut down for weeks until more safeguards were added. A firmer legal footing, based on a stronger consensus, would have avoided this potentially dangerous gap in coverage.
* ***The program was leaked to the press,*** something the Administration claims has hurt our national security. We do not know who may have provided reporters with information about the program, but there were reports that some information may have been provided by professionals at NSA or DoJ who were extremely troubled by what they believed was an illegal program. Had the program been placed on a more solid legal footing, these dedicated professionals may not have felt compelled to seek outside oversight.
* ***Prosecutions may be jeopardized.*** Prosecutions that were based in any way on information obtained by this program may now be jeopardized if a court finds that the information was collected or used improperly. A more solid legal basis could have avoided this risk.
* ***Damaging impact on intelligence professionals.*** The legal uncertainty of this program (1) puts the men and women who were conducting this surveillance program, and those who were using the information, in jeopardy of potential criminal liability, (2) hurts agency morale, and (3) may well undermine officials' confidence that they can and should carry out future presidential directions without facing potential liability. (The same is true for the torture debate--where intelligence officials operated pursuant to a DOJ memo that was later repudiated when it

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00227 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.160

became public. How are the folks on the front line of intelligence supposed to react to all of this?)

* ***Diverted vital investigative resources.*** There are indications that this program produced too many false leads and may have led to an unproductive diversion of important FBI resources that could have been better used conducting more fruitful investigations of suspected terrorist activity inside the US. For example, press reports indicate that only about 10 intercepts each year—out of the thousands of communications intercepted through this program-- proved suspicious enough to justify intercepting all the domestic communications of the US-end of the original communication. Presumably, the rest of the intercepted communications with Americans ultimately proved to be unrelated to terrorism and involved innocent Americans or others inside the US.

* ***Complicates future efforts to gain the support of Congress.*** The expansive reading of the AUMF may make it harder to get such authorizations in the future, potentially weakening public support for future conflicts. Indeed, the mistrust created on both sides of the aisle in Congress may impact executive branch efforts in a number of ways beyond just authorizations for the use of force.

Ensuring appropriate safeguards in FISA is essential to avoiding similar national security problems in the future and, ultimately, to defeating the terrorists. The bottom line is that the best way to be strong on terrorism is not to defer to the avaricious accumulation of power by the Executive branch but to better understand the true nature of the long term struggle against violent extremists. We can only defeat this threat by building upon the strengths of our system. That city on the hill can outshine the twisted but compelling lure of violent jihad. That is how we will ultimately prevail.

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00228 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.161

SENATE COMMITTEE ON THE JUDICIARY

Hearing on

"Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?"

Tuesday, September 25, 2007

Testimony of Michael A. Sussmann
Partner, Perkins Coie LLP:

Perspective of Communications Providers on the Protect America Act of 2007

Chairman Leahy, Ranking Member Specter, and Members of the Committee, thank you for this opportunity to provide testimony concerning providers' perspectives on FISA modernization, the Protect America Act of 2007 (the "Act"), and upcoming efforts to renew and amend national security legislation.

I am a partner in the Washington, DC office of Perkins Coie LLP. We represent a large number of fixed-line (telephone), wireless, and Internet service providers in responding to government demands for customer information and electronic surveillance. I have a current national security clearance and I counsel providers on compliance with the Foreign Intelligence Surveillance Act (FISA) and orders issued from the Foreign Intelligence Surveillance Court, national security letters, and other issues relating to national security. Prior to joining Perkins Coie, I was at the Department of Justice for 12 years, handling national security issues for the Assistant Attorney General for the Criminal Division and then, for eight years, as a senior counsel in the Computer Crime and Intellectual Property Section. My testimony today is based on my own views and experience and does not represent the views of any particular communications provider.

The Role of Communications Providers Under FISA

Communications providers have a critical role to play in the implementation of FISA and other foreign intelligence surveillance legislation. Providers receive classified orders from the FISA Court; review the orders and consider their legality and practicality from a technical standpoint; and decide whether to comply with an order or seek modification or clarification from the FISA Court or the government. Notwithstanding the valuable perspective of the privacy community and others in academia, outside the federal government no one other than the providers see or will see FISA orders or directives under the Protect America Act. Indeed, section 105B(h) of the Act provides specific authorization for *providers* alone to challenge before the FISA Court the legality of a directive issued under the Act. It is therefore important that providers' perspectives be considered when FISA is amended or when new legislation in this area is considered. Clarity is essential and will reduce the likelihood of disputes, delay in responding to directives or orders, and filing of petitions.

53358.162

Providers' Perspective on FISA and FISA Modernization

When passed in 1978, the Foreign Intelligence Surveillance Act was critical in overlaying federal court supervision and specific procedures onto the government's ability to conduct national security investigations that involved U.S. persons. The protections contained in FISA not only provide the supervision of a neutral and independent Article III judge, they provide legal standards and regularized procedures that allow providers to know they are keeping within the law and hewing to the intent of Congress.

Providers therefore must rely on the President and Congress to forge the necessary legal tools for national security investigations and to balance those needs with the protections guaranteed by the Constitution and by statute, and with general notions of privacy and individual liberty. With clear guidance in the form of legislation, providers have for almost 30 years complied with the signed orders from federal judges appointed to the FISA Court. The clarity in FISA and in the instructions from the FISA Court has allowed providers to offer lawful assistance in national security investigations that required access to electronic communications.

While providers understand the needs that the Protect America Act is intended to address, a number of provisions contained therein are either ambiguous or are subject to differing interpretations. Since the Act sunsets six months after its enactment, and leaders in Congress and executive branch have discussed the issue of its renewal or amendment, I would like to summarize for the Committee eight issues from the Protect America Act that would benefit from clarification in any future legislation that would seek to renew or amend the Act.

Eight Issues From the Protect America Act That Would Benefit From Clarification

1. Does the Protect America Act authorize through the use of directives the production of *stored* communications (e.g., email mailboxes) from providers, as opposed to just the real-time interception of communications?

Notably, the Act uses the terms "acquisition" and "acquisition of foreign intelligence information" throughout, including for each of the five criteria for a certification in section 105B(a), and in the description of a directive in Section 105B(e). By way of analogy, in the criminal context, the term "acquisition" is used in the federal Wiretap Act, 18 U.S.C. § 2510, but not the Stored Communications Act, 18 U.S.C. § 2701. The term "intercept" is defined in the Wiretap Act as "the aural or other *acquisition* of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (emphasis added). The same usage can be found elsewhere in the statute (*see* 18 U.S.C. § 2511(2)(f): "Nothing contained in [the Wiretap Act] or . . . the Communications Act of 1934, shall be deemed to affect the *acquisition* by the United States Government of foreign intelligence information from international or foreign communications . . . ." (emphasis added)). However, the Stored Communications Act, which deals exclusively with the disclosure (to the government or third parties) of stored communications, does not use the term "acquisition," instead using

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00230 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.163

such terms as "divulge" or "disclose" "the contents of a communication *while in electronic storage*."

Notwithstanding the plain language in the law, case law does exist that interprets the term "acquisition" to include stored communications. Since disclosure under the Protect America Act of stored communications could involve access to entire email mailboxes or other account content, as opposed to just individual email messages or documents, the question of applicability of the Act to stored communications and content certainly is one that should be answered in clear and unambiguous terms, especially if the account creation and use predates the time when the government reasonably believed that the surveilled person was located outside the United States.

2. Does the Protect America Act authorize through the use of directives physical searches and "section 215 orders" for production of business records, since physical searches and section 215 orders are not considered "electronic surveillance" under FISA as it existed before passage of the Protect American Act?

Section 105B(a)(2) of the Act requires certifications to the FISA Court concerning directives to contain determinations by the Director of National Intelligence ("DNI") and the Attorney General that "the acquisition does not constitute electronic surveillance." Neither physical searches authorized under FISA at 50 U.S.C. §1822 nor the compelled disclosure of business records authorized at 50 U.S.C. § 1861 (often referred to as "section 215 orders" because of the section of the USA Patriot Act that created this power) fall under FISA's definition of electronic surveillance at 50 U.S.C. § 1801(f). Therefore, if the DNI and Attorney General make the *other* determinations required by sections 105B(a)(2)-(5), directives arguably could include demands for physical searches and for business records.

I note that in testimony last week before the House Judiciary Committee, Ken Wainstein, Assistant Attorney General for the National Security Division of the Justice Department, took the position that the Act does not authorize physical searches of the homes, businesses or effects of persons located in the United States. He further stated that the Administration would not take advantage of any authorization under the Act to demand business records.

Notwithstanding the positions offered by Mr. Wainstein, I believe the Act as written could allow for such searches and demands for records which, in turn, could be a basis for the compelled disclosure by providers of stored communications. For this reason, it would be preferable for any new legislation in this area to address the availability of physical searches and demands for business records under the Act.

3. Whose "reasonable belief" concerning the location of parties to a communication is contemplated in section 105B(a)(1) of the Protect America Act – only that of the U.S. intelligence community or that of providers, as well?

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00231 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.164

If a directive were to require surveillance on 20 target accounts, and a provider were able to ascertain that five of those accounts contained and involved only domestic communications, surveillance of those five accounts would constitute "electronic surveillance" and would not be authorized under the Protect America Act. It would be instructive to providers to know whether they can "look behind" a directive and comply with regard to only those accounts (in this case 15 of 20) for which a reasonable belief as to an international connection exists. In some cases it may be obvious to a service provider, such as when a target call is registered on a cell site within the United States; and in other cases, it may be clear from network information that the target was accessing a system from within the United States if such information was analyzed. Service providers do not want technical mandates, but they also do not want to be liable if the "reasonable belief" turns out to be incorrect. A clearer articulation of this standard would benefit all stakeholders.

4. Does the requirement that a certification be based on a determination that "a significant purpose of the acquisition is to obtain foreign intelligence information" provide any *real* limitation in the breadth of surveillance?

If technically feasible, a directive requiring surveillance of all communications to or from a particular foreign country would appear to be lawful if the U.S. government was looking for the communications of just one terrorist, as it could be said that a *significant purpose* of that acquisition would be to obtain foreign intelligence information. For this reason, a limitation for overbreadth may be advisable. To achieve this goal, Congress may want to consider amending section 105B(a)(4) to say that "a significant purpose of the acquisition is to obtain FII *and the collection is not overly broad.*"

To be clear, providers are not in a position to assess the purpose of an acquisition, nor should they be. But overbreadth is a significant concern for service providers as it creates technical burdens, which I discuss below. Further, since minimization under FISA is *post hoc*, meaning that everything is collected and only relevant communications are reviewed, the practical consequences of overbroad surveillance include the collection and retention of large quantities of "innocent" communications.

5. Does a provider get notice of the government's motion to compel compliance with a directive under section 105B(g) of the Protect America Act, and thereby a chance to respond to such motion, or can the government's motion be filed with the FISA Court on an *ex parte* basis with a provider only learning of the government motion upon issuance of an order by the FISA Court?

While traditional government practice before the FISA Court has been limited to *ex parte* filings and appearances, the Protect America Act authorizes (a) providers to challenge before the FISA Court the legality of a directive, and (b) the government to seek assistance from the FISA Court in compelling compliance on the part of a provider. However, the Act only provides procedures in the former case. Where providers are unable to comply with the requirements under a

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00232 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.165

directive, it is important that they have the ability to present their positions to the FISA Court, should the issue of provider compliance be presented to the FISA Court by the government.

6. In *non-emergency* cases, can directives be issued to communications providers orally, and what information should be required to be in any written directives?

Section 105B(e)(1) of the Protect America Act authorizes the DNI and Attorney General to "direct a person to immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition." However, there is no mention in the Act as to whether this direction should come in the form of a specific writing, or whether communications that are solely oral would be acceptable.

Providers would like any directives issued under the statute to be presented to providers in the form of a writing. Oral directives do not provide a clear record of a government request, and for obvious reasons they can lend themselves to misunderstandings.

Moreover, as both the federal Wiretap Act and the Pen Register and Trap and Trace statute provide instruction as to what details must be included in any order presented to a provider, Congress may want to consider whether it should include in any future amendments to FISA requirements for certain information to be included in a directive. For example, information such as the statutory authorization, reference to a certification by the FISA Court, a declaration that all assistance requested does not constitute electronic surveillance, and the maximum number of simultaneous surveillance contemplated by the directive may be helpful. Such specificity might enhance accountability and set clearer limits on the surveillance authorized under a directive.

7. What are the limits to the burdens placed on providers by directives, and can a directive require changes to service and/or architecture to accomplish surveillance, so long as costs are paid?

Section 105B(f) of the Protect America Act provides that the "Government shall compensate, at the prevailing rate" a provider for compliance with a directive. Providers are nonetheless concerned about their ability to comply with a directive which is overly burdensome or which requires interference with or changes to its network infrastructure or provision of service.

A provider compliance center that can support 20 simultaneous interceptions in the criminal context will not necessarily be able to support a request in a directive to run 100 – both from the standpoint of personnel and equipment. Likewise, a provider's network simply may not be built to intercept certain communications, such as peer-to-peer text messaging. While many courts have addressed issues of undue burden in government requests, the Protect America Act is silent on this point. A notion of fairness could be added in section 105B(h)(1)(A) by inserting a reference to burden such as the following: "A person receiving a directive issued pursuant to subsection (e) may challenge the legality *or undue burden* of that directive by filing a petition . . . ."

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00233 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.166

8. Finally, since the immunity provision in the Protect America Act is not severable from the remainder of the statute, would immunity survive a FISA Court finding that the Act is unconstitutional?

Section 105B(l) states that "notwithstanding any other law, no cause of action shall lie in any court against any person for providing any information, facilities, or assistance in accordance with a directive under this section." Because of the public interest in and controversy surrounding FISA and warrantless surveillance, it is not unlikely that a plaintiff will challenge the constitutionality of the Protect America Act or any successor legislation. Providers who, in good faith, comply with a directive would nonetheless lose the protection of section 105B(l) immunity if they are later sued and the statute were previously found to be unconstitutional.

Courts might be inclined to extend this immunity, and indeed good public policy requires such protection, for it is in the interest of all three branches of our government for citizens to accept the legality and force of any law properly enacted; second-guessing the *future* effect of a law in fact undermines the rule of law. A provision in an amended Protect America Act that makes the immunity provision severable in the event of a finding of unconstitutionality benefits the executive branch in removing hesitancy in compliance with directives, Congress by giving more certainty to the effect of its laws, and the courts in reducing unnecessary litigation over the existence of immunity.

Conclusion

As I discussed earlier, communications providers have a critical role in facilitating lawful access to electronic communications in national security investigations. As intermediaries between government authorities and subjects of surveillance, they ensure that surveillance laws are followed.

I am grateful to have had this opportunity to provide a perspective from industry on FISA and FISA modernization, and to highlight certain ambiguities in the Protect America Act that Congress may want to consider when crafting any future legislation. It is imperative that these laws are as clear and unambiguous as possible. The views I expressed today are of course my own, and I cannot claim to represent all or even a majority of industry views. Nonetheless, my hope is that the deliberations of this Committee will be aided by inclusion of industry's perspectives along with other viewpoints on this topic.

###

VerDate Nov 24 2008 10:49 Nov 30, 2009 Jkt 053358 PO 00000 Frm 00234 Fmt 6633 Sfmt 6011 S:\GPO\HEARINGS\53358.TXT SJUD1 PsN: CMORC

53358.167