AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 110–882

FISA AMENDMENTS: HOW TO PROTECT AMERICANS' SECURITY AND PRIVACY AND PRESERVE THE RULE OF LAW AND GOVERNMENT ACCOUNTABILITY

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

OCTOBER 31, 2007

Serial No. J–110–59

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

52–426 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 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00001 Fmt 5011 Sfmt 5011 S:\GPO\HEARINGS\52426.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 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00002 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\52426.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 114
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont 1
prepared statement 126
Specter, Hon. Arlen, a U.S. Senator from the State of Pennsylvania 3

WITNESSES

Black, Edward, President & CEO, Computer & Communications Industry Association, Washington, D.C. 45
Halperin, Morton H., Director of U.S. Advocacy, Open Society Institute, Washington, D.C. 49
Philbin, Patrick F., Partner, Kirkland & Ellis, Washington, D.C. 47
Wainstein, Kenneth L., Assistant Attorney General, National Security Division, U.S. Department of Justice 6

QUESTIONS AND ANSWERS

Responses of Edward Black to questions submitted by Senator Brownback 56
Responses of Morton Halperin to questions submitted by Senator Brownback . 59
Responses of Patrick Philbin to questions submitted by Senator Brownback 65
Responses of Kenneth Wainstein to questions submitted by Senators Leahy, Feingold, Kennedy, and Kyl 69

SUBMISSIONS FOR THE RECORD

American Library Association and the Association of Research Libraries, Washington, D.C., letter 91
Black, Edward, President & CEO, Computer & Communications Industry Association, Washington, D.C., statement 94
Burgess, Ronald L., Jr., Lieutenant General, Office of the Director, National Intelligence, Washington, D.C., letter 104
Dodd, Hon. Christopher J., a U.S. Senator from the State of Connecticut, statement and letter 108
Department of Justice, John D. Ashcroft, Jack Goldsmith, James B. Comey and Patrick F. Philbin, Washington, D.C., letter 112
Halperin, Morton H., Director of U.S. Advocacy, Open Society Institute, Washington, D.C., statement 115
Philbin, Patrick F., Partner, Kirkland & Ellis, Washington, D.C., statement ... 128
Sorrell, William H., Vermont Attorney General, G. Steven Rowe, Maine Attorney General, Richard Bluenthal, Connecticut Attorney General, Anne Milgram, New Jersey Attorney General, and Robert M. Clayton, III, Commissioner, Missouri Public Service Commission, letter 139
Wainstein, Kenneth L., Assistant Attorney General, National Security Division, U.S. Department of Justice, statement 143
Wall Street Journal, Benjamin Civiletti, Dick Thornburgh and William Webster, October 31, 2007, article 164

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00003 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

FISA AMENDMENTS: HOW TO PROTECT AMERICANS' SECURITY AND PRIVACY AND PRESERVE THE RULE OF LAW AND GOVERNMENT ACCOUNTABILITY

WEDNESDAY, OCTOBER 31, 2007

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

The Committee met, pursuant to notice, at 10:10 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Feinstein, Feingold, Durbin, Cardin, Whitehouse, Specter, Hatch, Kyl, Sessions, Graham, Cornyn, Brownback, and Coburn.

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

Chairman LEAHY. The Foreign Intelligence Surveillance Act, or FISA, is intended to protect both our national security, but, also, the privacy and civil liberties of Americans.

Changes to that law have to be considered carefully and openly. They can't be eviscerated in secret administration interpretations or compromise through either fear or intimidation.

The so-called "Protect America Act," passed just before the summer recess, was an example of the worst way possible to amend FISA. It was hurriedly passed under intense partisan pressure from the administration and provides sweeping new powers to the government to engage in surveillance without warrants of international calls to and from the United States involving Americans.

It provided no meaningful protection for the privacy and civil liberties of the Americans who are on those calls.

Now, this Act will expire next year. So this is the committee's second hearing to inform our consideration of possible legislation to take the place of that flawed Act.

Of course, we have to accommodate legitimate national security concerns and the need for flexibility and surveillance of overseas targets, but Congress should do that in a way that protects the civil liberties of Americans.

I commend the House committee and I commend the Senate Select Committee on Intelligence for seeking to incorporate the better ideas from our work this summer into the current legislative proposals.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00005 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

The House of Representatives is considering the RESTORE Act, which appears to take a fair and balanced approach, allowing flexibility for the intelligence community, while providing oversight and protection for Americans' privacy.

The Senate Select Committee on Intelligence has also reported a bill that makes improvements to the current temporary law. Increasing the role of the FISA Court and oversight by the Inspector General and the Congress are matters we should have incorporated this summer.

At the outset, I should acknowledge the grave concern I have with one aspect of S. 2248. It seems to grant immunity or, as Senator Dodd called it, "amnesty", for telecommunications carriers for warrantless surveillance activities from 2001 through this summer. Those seem to be, on the face of them, at least, contrary to FISA and in violation of the privacy rights of Americans.

Before even considering such a proposal, as we said at the Mukasey hearing, a matter that will be before our committee, I think, next Tuesday, Senator Specter and I have always been clear with the administration that we would need the legal justifications, authorizations and other documents to show the basis for the action of the government and the carriers.

And since the existence of the President's secret wiretapping program became public in December 2005, this committee sought to have relevant information through oral and written requests and by conducting oversight hearings.

After our repeated requests did not yield information the committee requested, we authorized and issued subpoenas for documents related to the legal justification for the President's program.

Finally, this week, the administration, belatedly, responded. Senators on the committee and designated staff have begun to receive access to legal opinions and documents concerning authorization and reauthorization of the program. It's a significant step and it was long overdue.

I insisted that all members of the committee have access, Republicans and Democrats alike, and that was agreed to in a meeting yesterday, and I am considering carefully what we're learning from these materials. The Congress should be careful not to provide an incentive for future unlawful corporate activity by giving the impression that corporations violate the law and disregard the rights of Americans. They'll be given an after-the-fact free pass.

If Americans' privacy is to mean anything and if the rule of law is to be respected, I think that would be a wrong result. A retroactive grant of immunity, or amnesty, or preemption of State regulators does more than let the carriers off the hook.

Immunity is designed to shield this administration from any accountability for conducting surveillance outside the law. It would make it impossible for Americans whose privacy has been violated illegally to seek meaningful redress.

Lawsuits would be dismissed as a result of such a grant of immunity, and perhaps as the only avenue that exists for an outside review of the government's program and honest assessment of its legal arguments, especially as the Congress has, for years, been stonewalled on this program. That kind of assessment is critical if our government is to be held accountable.

One of my chief inquiries before deciding to support any legislation on the subject is whether it's going to bring about government accountability. Anyone who proposes letting the telecommunications carriers off the hook or preempting State authorities or giving the type of immunity or amnesty has a responsibility to propose a manner to test the legality of the government's program and decide whether it did harm to the rights of Americans.

Safeguarding the new powers we are giving to our government is far more than just an academic exercise. FISA law itself is a testament to the fact that unchecked government power leads to abuse.

The FISA was enacted in the wake of earlier scandals, when the rights and privacy of Americans were trampled because nobody was watching.

We in the Senate, and this committee especially, have a solemn responsibility to 300 million of our fellow citizens because the American people's rights and freedom and privacy can be easily lost, but once lost, they're very difficult to win back.

So I look forward to the testimony of our witnesses. I appreciate them being here.

I will yield to Senator Specter.

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

Senator SPECTER. Thank you, Mr. Chairman. I am glad to see that we have come a long way in the last 18 months since legislation was introduced in mid-2006 to bring the terrorist surveillance program under the FISA court, and we have some very important considerations to protect U.S. persons, to have the FISA court review the procedures and to handle minimization in an appropriate way.

With respect to the request for retroactive release of liability, I have great reluctance. Part of that stems from the secrecy that the government has interposed when we were seeking subpoenas last year for the telephone companies. We were thwarted by action of the Vice President in contacting Republican members, without notifying the Chairman, and, as I see the situation, I think the telephone companies do have a strong, equitable case, but my inclination is that they ought to get indemnification, if the court sought not to be closed.

I doubt very much the cases will be proved, but if plaintiffs can prove them I think they ought to have their day in court. And it is costly, but that's part of the cost of the war on terrorism.

Finally, yesterday, we had a closed-door briefing on what is happening, and I believe we need more briefings. The government has been reluctant to follow the statute on informing the Intelligence Committee about FISA until they needed support for the confirmation of General Hayden as Director of the CIA. And the session we had yesterday was an important one and I think we need more information from the administration.

The Chairman has referred to the pendency of the nomination of Judge Mukasey to be Attorney General and that is a matter which covers the issues which are before us now, or a first cousin, at a very minimum.

And it is my hope, Mr. Chairman, that we would be able to resolve the issues on Judge Mukasey sooner rather than later, and I know that's your inclination, as well. You had wanted to bring the matter to a determination by the committee early.

I think it may be advisable to have a closed-door session, where we talk about water-boarding and we talk about torture and we talk about those techniques. Earlier this week, in the wake of the issue on water-boarding, I had an extensive briefing by General Hayden. There are people who overlap on the Intelligence Committee with the Judiciary Committee, who know about the details, and I believe it is a matter that the full committee ought to be informed about.

I think that the extensive letter which Judge Mukasey has submitted goes about as far as he can go. He has repudiated water-boarding, he has rejected it, but he has stopped short of making a determination of legality. And let's face the facts. The facts are that an expression of an opinion by Judge Mukasey prior to becoming Attorney General would put a lot of people at risk for what has happened.

Now, they may be at risk regardless of what Judge Mukasey says or what the next Attorney General says. And last week, former Secretary of Defense Rumsfeld was in France and there was an effort made to initiate a prosecution against him, and extraterritorial jurisdiction is being asserted by many countries under the Doctrine of Crimes Against Humanity.

Ordinarily, a prosecution can be brought only where the act occurred, but what Judge Mukasey would say on that subject has repercussions in that direction.

The standard has been articulated of whether it shocks the conscience under the Rochin decision, and that depends upon a totality of circumstances. It depends on who is the individual, what access the individual has to information, how important the threat is, what is the likelihood of getting information which would be critical in saving lives.

We all dodge around the so-called "ticking bomb" case. Nobody wants to articulate a principle if there are any exceptions to torture, and it is probably advisable not to be explicit in that situation because you may make exceptions which will be broadened; as the expression goes, you can "drive a truck through."

But we do know that the Department of Justice is in dire straits. If there's one thing that this committee, and perhaps the entire Senate, is unanimous on, it's that the Department of Justice is dysfunctional.

I think we need extensive assurances. But as I carefully read Judge Mukasey's letter, I don't know how much more he could say than what he has said, considering the exposure to people in collateral circumstances and considering the impossibility of predicting what may be faced with respect to a future potential danger if the so-called "ticking bomb" hypothetical were to reach fruition.

But what I would like to see is us, Mr. Chairman, go into a closed session, like we had yesterday. I thought it was very fruitful when we were behind closed doors and could talk more openly about the subject matter of what the telephone companies have been doing and to share information from those who know more

about the interrogation techniques and the water-boarding than many members of this committee know.

The Intelligence Committee is privy to that, and they should be, but so should this committee, when we have to make a measurement and make a decision about the adequacy of what Judge Mukasey has said on a subject which could defeat his confirmation.

No doubt, the confirmation is at risk at this moment because he has not answered the question categorically, and I think we need to have a very frank discussion, with more facts available, and I believe that can only be done in a closed-door session.

I would hope we might do that early next week. Hopefully, we could get Judge Mukasey on the agenda for next week and either fish or cut bait on this important matter.

Chairman LEAHY. As I said, Judge Mukasey will be on the agenda on Tuesday, but I think there are a whole lot of—and the reason I'm doing it Tuesday and not Thursday is because—and, of course, everybody's rights are protected under that—there are a whole lot of other issues that he responded to late last night involving, among other things, executive authority, his views on the ability of the executive to override laws passed by Congress, his views on the executive being able to preempt congressional actions on contempt citations and things like that that others want to consider.

So it's not just the water-boarding issue. Obviously, many of us felt that the United States, which would roundly and universally condemn the water-boarding of an American held by any other country, many of us had felt that the Attorney General nominee should do the same thing.

It would put us back just to think, without even taking current times, to the old Soviet Union days. If the then-Soviet Union had picked up an American, water-boarded that American, you'd have 535 Members of the Congress, House and Senate, who would vote for a resolution condemning that, and whoever was present, Democratic or Republican, would have condemned it.

That is one of the concerns I hear expressed by Americans. But let's not go into debate on that. We will have plenty of time to debate this issue. That's why I'm setting aside a special time just for this matter.

We have before us Kenneth Wainstein, who served as the First Assistant Attorney General for National Security since September 2006. I'm sure he thinks that time has gone by so rapidly.

Prior to this appointment, he has held various positions in the Justice Department, including as the United States Attorney for the District of Columbia, where we first met. When I say that, I hasten to add, not because I or any member of this committee was before him in that capacity. He also served as chief of staff to the Director of the FBI, where we also had dealings.

Mr. Wainstein, would you please stand and raise your right hand?

[Whereupon, the witness was duly sworn.]

Chairman LEAHY. Of course, your full statement will be made part of the record, but, please, go ahead.

STATEMENT OF KENNETH L. WAINSTEIN, ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY DIVISION, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. WAINSTEIN. Thank you, sir. Chairman Leahy, Ranking Member Specter, members of the committee, I want to thank you all for this opportunity to testify before you on this important matter. I'm proud to be here to represent the Department of Justice and to discuss our views on this very important issue with you.

I'd like to take a few minutes just to discuss three specific points. I'd like to explain, first, why it is I believe that Congress should permanently legislate the core provisions of the Protect America Act; second, how it is that we've gone about implementing the authority in the Protect America Act with significant oversight mechanisms and congressional reporting; and, third, I'd like to give you our preliminary views on the thoughtful bipartisan bill that was reported out of the Senate Intelligence Committee 2 weeks ago.

Before I do that, I'd like to express our appreciation for the attention that Congress has given to this important issue. Congress has held numerous hearings and briefings on the issue over the past year or so and that process has produced the Protect America Act, which was a very significant step forward for national security, and in the Senate, it culminated in a bipartisan bill referred to this committee, S. 2248, which was voted out on a strong 13–2 vote.

We applaud Congress for its initiative on this issue and its willingness to consult with us as it moves forward on FISA modernization.

Let me turn to why I believe that the core provisions of the Protect America Act need to be made permanent.

The government's surveillance activities are a critical, if not the most critical part, of our investigative effort against international terrorists and other national security threats. By intercepting these communications, we get an insight into their capabilities, their plans, and the extent of their networks.

Before the Protect America Act, however, our surveillance capabilities were significantly impaired by the outdated legal framework in the FISA statute. FISA established a regime of court review for our foreign intelligence surveillance activities, but not for all such activities.

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

While this construct worked pretty well at first, with the vast changes in telecommunications in the past 29 years, a good number of our surveillances that were originally not intended to fall within FISA became subject to FISA, those which are targeted outside the U.S., which required us to go to court to seek authorization and effectively conferred quasi-constitutional protections on terrorist suspects and other national security threats who are overseas.

Over that same period, we were facing an increasing threat from Al Qaeda and other international terrorists and it was the combination of these two factors, the increasing burden of FISA and

the increasing threat, that brought us to the point where we needed to update FISA.

In April of this year, we submitted to Congress a comprehensive proposal to modernize FISA. As the summer progressed, Congress recognized the immediate need to address the rising threat and passed the Protect America Act, which clarified that overseas surveillances are not subject to FISA Court review. And within days, we implemented that new authority and the DNI has announced that we've filled the intelligence gaps that were caused by FISA's outdated provisions.

We've recognized, from the very moment that the Protect America Act was passed, that Congress would reauthorize this authority only if we could demonstrate to you and to the American public that we can, and will, exercise this authority responsibly and conscientiously.

To that end, we imposed oversight procedures upon ourselves that are well beyond those required in the statute and we committed to congressional reporting that's well beyond that required in the statute, and in the process we've established a track record of responsible use of the Protect America Act, a track record that provides solid grounds for Congress to permanently reauthorize it.

Against that backdrop, the Senate Intelligence Committee recently voted out S. 2248. And we're still reviewing the bill, but we believe that it's a balanced bill that includes many sound provisions. It would allow our intelligence professionals to collect foreign intelligence against targets located overseas without obtaining prior court approval, and it also provides retroactive immunity to electronic communications service providers who assisted the government in the aftermath of 9/11.

We believe this immunity provision is necessary, both as a matter of fundamental fairness and as a way of ensuring that providers will continue to provide cooperation to our surveillance efforts.

That bill also remedies the possible over-breadth concerns that some had regarding the Protect America Act, and it includes significant oversight and reporting mechanisms.

We do, however, have concerns about certain provisions in the bill; in particular, the sunset provision and the provision that would extend the role of the FISA Court, for the first time, outside our borders by requiring a court order when we surveil a U.S. person who is acting as an agent of a foreign power outside the U.S.

However, we look forward to working with this committee and Congress to address those concerns and to seize this historic opportunity to achieve lasting modernization of FISA that will improve our ability to protect both our country and our civil liberties.

Thank you for the opportunity to testify, and I look forward to answering your questions.

Chairman LEAHY. Well, thank you for your statement.

[The prepared statement of Mr. Wainstein appears as a submission for the record.]

Chairman LEAHY. When you deal with something like this, it's very difficult to be sure what parts we're dealing with in open session, but the Senate Intelligence Committee, in their report on their legislation, said that the government provided letters to elec-

tronic communication providers at regular intervals between late 2001 and early 2007 to justify the existence in this program of warrantless wiretapping.

All these letters stated the activity has been authorized by the President. All but one stated the activities had been deemed lawful by the Attorney General.

So is it the position now of the government that these letters were certifications that made it legal for the companies to assist the government?

Mr. WAINSTEIN. Those letters were the assurances that were provided to the companies that this was a program directed or authorized by the President and that they were legal, and if you look at the criteria in the retroactive immunity provision in the Senate Intelligence bill, those criteria are satisfied.

Chairman LEAHY. If they said that this would make it legal, why is it necessary to provide immunity? Wouldn't it be just better, maintaining faith in government, to let our judicial system make that determination?

I mean, the government has already told the carriers that this was legal. Why do we need to do further? Shouldn't the courts be allowed now to say whether the government was right in saying that?

Mr. WAINSTEIN. Well, I understand the sentiment that we should be allowed to go—people who feel like they are aggrieved should be allowed to go into court and, as a standard matter, that makes sense.

The problem here is that, sort of as I alluded to earlier, there's a basic fundamental matter of fairness that the government, at the highest levels, in the aftermath of the worst attack upon the United States, at least since Pearl Harbor, went to these providers, who are the only ones who can provide the assistance for critical communications intelligence work—went to them, said, "We need this work. It's lawful. It's been deemed lawful at the highest levels of the American government and we need that assistance."

Chairman LEAHY. I accept that. But so why shouldn't that be enough? Why do you have to pass further legislation?

If you feel secure in what you did, why ask for further legislation? Why not let the courts just deal with the certification made by the President that this was legal?

Mr. WAINSTEIN. Well, we feel that it's unfair to—

Chairman LEAHY. Unless you're not comfortable with having made that certification.

Mr. WAINSTEIN. No. And I don't believe the concern is airing out what the government did or didn't do. The concern is airing out what the companies did and putting them through the cost, litigation, the exposure, the difficulty of litigation, when they were really just doing what they did to protect the country.

If there are to be lawsuits, they should be against the government. The problem with any lawsuits against the companies is that it's unavoidable that very sensitive classified information is going to be released, and we've seen this already in this litigation.

Chairman LEAHY. If you make a blanket assertion of state secrets, then you do have difficulty. But if you're just going to use

the specific classified information needed, that's done by courts all the time. The classified information is looked at in camera.

Why couldn't that be done here?

Mr. WAINSTEIN. That's right, but in my experience, the classified information that's subject—

Chairman LEAHY. You had that as U.S. Attorney.

Mr. WAINSTEIN. Yes. Yes. And there is a standard—there's CIPA, the statute that allows the government to use classified information to bring a prosecution that implicates classified information and insulate from unwarranted disclosure.

The problem is that the whole cause of action here, the whole sort of mode of conduct being challenged is a highly classified program and our adversaries—our adversaries, they're not ignorant. They know that this is going on and they know to watch what's happening in the news, because they want to get tips as to how it is we're trying to surveille them, and the adversaries aren't just terrorists in caves. They're also potentially foreign services that are pretty sophisticated. So every little nugget of information that comes out in the course of these litigations helps our enemies.

In addition, I would say you've got to also keep in mind—

Chairman LEAHY. So should we be prosecuting—if that's the case, be prosecuting the New York Times and others for having printed all this? I mean, they gave the information.

Actually, Congress found out about the things that were supposed to have been reported to Congress and never was. We read it on the front page of the New York Times.

Mr. WAINSTEIN. No. I'm not advocating prosecutions—

Chairman LEAHY. I didn't think so.

Mr. WAINSTEIN.—in that realm. What I'm saying, though, is that there are serious concerns on the part of—

Chairman LEAHY. In my experience, I've only had one government official recommend or say they wanted to investigate the New York Times and prosecute them, and that person is no longer alive.

Go ahead.

Mr. WAINSTEIN. Also, I'd direct your attention to the fact that these providers—I can't go into exactly which providers they were—but you could imagine that these are companies that might well have personnel and facilities around the world and they've got a very serious concern that if they get identified, intentionally or unintentionally, through litigation, those facilities, those personnel might well be subject to risk, because they have been identified as assisting us in our efforts against terrorists.

Chairman LEAHY. For those who think that there should be some accountability on the part of our government, and obviously the government did not want to have that accountability, they did not go to the people in even the Congress, where there may be a check-and-balance, acted totally outside of any kind of accountability, until somebody within your administration leaked all this to the press.

Isn't there some way—how do you find a way to assess the legality and appropriateness of this warrantless wiretapping program?

If you say we can't have court cases, we've got to have immunization, how do you assess this?

Mr. WAINSTEIN. Well, I think that if there are to be lawsuits—I mean, the concern people have here is with the legality of the program and that legality determination was made by the government.

So if people have a concern about it, it should be—any litigation should be directed at the government.

Chairman LEAHY. Okay. But then you have a catch-22. The government says, "Ah, state secrets."

Mr. WAINSTEIN. Right, which we would say in the context of litigation against the carriers, as well, which is—

Chairman LEAHY. But you're going to say it against the government. So there really is no way to find the government accountable.

If we give blanket amnesty to the companies, then you're not going to be able to sue the government. They're going to provide their own amnesty by saying "state secrets".

Mr. WAINSTEIN. And we're in that position right now. No matter whether the litigation is directed at the companies or at the government, state secrets can be interposed.

Keep in mind, there are numerous—

Chairman LEAHY. Why? Why can't they just go to classified information, take it in camera?

Mr. WAINSTEIN. Well, we have to demonstrate that—I mean, we have to go and demonstrate that state secrets are going to be implicated here, that the litigation can't go forward without divulging state secrets, and we invoke the doctrine.

But keep in mind, if I may, Mr. Chairman, there are many investigations going on right now about the propriety of what was done or not done under the terrorist surveillance program.

So in terms of accountability, if there is wrongdoing, that wrongdoing is being ferreted out in ways, very traditional ways, other than litigation.

Chairman LEAHY. I'm not sure of that, because it seems that you're putting up brick walls everywhere somebody might look at it.

Let me ask you one, and my final, question. The House is considering the RESTORE Act. They have a provision calling for the Department of Justice Inspector General to audit all government surveillance programs that occurred outside of FISA in the years following 9/11.

Now, they weren't audited. Even if we were to grant retroactive immunity to the telephone companies, do you object to Congress providing for such an audit in the bill that might go to the President?

Mr. WAINSTEIN. As I recall, the RESTORE Act provides or directs the Department of Justice Inspector General to do oversight—ironically, sort of oversight of intelligence community agencies—and we did have some concern about that, just because that's a little bit outside the DOJ/IG's lane; very strong Inspector General, I grant you, but outside his lane. So we had some concerns about that.

We also thought that injecting the whole terrorist surveillance program issue into this was unfortunate, because this is an effort, this being this legislation, is an effort to get Congress and the exec-

utive branch on the same page so that the constitutional issue of what can or can't be done under executive authority is not there.

Constitutionally, there's no pressure on that issue. So we think it's a better approach to say, okay, let's leave that aside in terms of whether the TSP was within the constitutional authority of the President or not, legal or not, and just focus on how we're going to fix FISA for the American people.

Chairman LEAHY. Maybe the difficulty is it seems so unprecedented for the administration to say they actually want to be on the same page with Congress—this administration anyway.

Senator Specter.

Senator SPECTER. Thank you, Mr. Chairman.

Mr. Wainstein, let's begin by discussing the relative role of the courts in protecting civil liberties and what it would mean to grant retroactive release of liability.

In the long history of this country, the courts have done a much better job in protecting civil liberties than has the Congress, from an overreaching executive branch, and we have seen, in this administration, extension of executive authority.

Now, in many ways it is necessary to protect America, and when the administration came to the Congress and asked for a Patriot Act, this committee took the lead in providing a Patriot Act with expanded executive authority for investigations to fight terrorism.

We, at the same time, imposed some limitations on oversight, negotiated with the administration, and then we found a signing statement which reserved the President's rights under Article 2, Commander in Chief, not to pay attention to the negotiated limitations.

And if we are to close the courthouse door to some 40 litigants who are now claiming that their privacy has been invaded, it seems to me we are undercutting a major avenue of redress.

If, at this late date, the Congress bails out whatever was done before and we can't even discuss what has been done, that is just an open invitation for this kind of conduct in the future.

Why not provide for indemnification? I believe the telephone companies have a very strong equitable case in saying that they were good citizens in responding to what the government ordered or requested and that the telephone companies shouldn't have to weigh the importance to national security.

But isn't the cost of those lawsuits part of our overall battle against terrorism, and isn't it infinitesimal cost, and isn't it likely that these lawsuits are not going to be successful?

You find the Federal Government interposing the Doctrine of State Secrets very broadly, trying to stop reviews under the terrorist surveillance program in the San Francisco Federal Court, or stopping litigants who have claimed torture on rendition can't go to court, can't have a hearing, because of the State Secrets Doctrine.

So it's a two-part question. Number one, why not make it a matter of indemnification, and isn't such indemnification really likely to cost the government very little, if anything, because these suits are destined for failure?

Mr. WAINSTEIN. I guess I would go back, Senator Specter. I'd go back to sort of the foundational issue for me, which is, these were

companies operating in good faith, on assurances from the government. If there is fault here, it's fault in the legal analysis and the decisions made by the government.

Senator SPECTER. I concede they're operating in good faith, and if they're indemnified, they're not going to be harmed. They're going to be held harmless.

So why not do that?

Mr. WAINSTEIN. True. I think you're right. It may be, as a legal matter, in terms of damages, they might be held harmless. But indemnification just means that we would pay the bills at the end of the process, but they'd have to go through the process.

And keep in mind, there is a lot of damage inflicted on these companies from having to go through the litigation, to be subject to discovery.

Senator SPECTER. What do they have to go through when you impose the State Secrets Doctrine? I can't even question you in a Judiciary Committee hearing about what has gone on, because it's a secret, and every time you impose the—virtually every time you impose the State Secrets Doctrine, you win. Those witnesses don't even have to appear. They're not going to be deposed. There's no discovery. They're cutoff at the pass, aren't they, really?

Mr. WAINSTEIN. Well, there's no assurance that we're going to prevail every time we interpose with the State Secrets Doctrine and the litigation still has to get to that point.

And keep in mind that we're also dealing with an industry that really has the access to the communications that we absolutely need and it's critical that we maintain cooperation with these companies.

If they find that they're constantly being pulled into courts for assistance with the government—

Senator SPECTER. Have you suggested to them that you would grant them indemnification?

When I've talked to the telephone companies and commented about that, they seem to think that that would answer the question.

Have you asked them?

Mr. WAINSTEIN. I know there have been discussions about various options—indemnification, substitution—but anything else to keep them out, anything that keeps litigation going also compromises secret information about sources and methods that we have a very serious concern about.

If we don't prevail with state secrets, then there's no guarantee that information is not going to get out. In fact, even just the filing of lawsuits and the allegations made can actually end up—allegations made in the initial pleadings can end up compromising sensitive sources and methods.

Senator SPECTER. Oh, really? Allegations in a lawsuit for people who are plaintiffs who don't have any inside information?

Mr. WAINSTEIN. Yes.

Senator SPECTER. If they know something, it must be in the public domain.

Let me move to one other line of questions, and that is to protect U.S. persons.

Admiral McConnell testified that there were 46 persons abroad, U.S. persons under surveillance abroad.

Why not require a showing of probable cause? And, also, on U.S. persons who are the recipients of calls from overseas? If you have a call from overseas to another overseas point going through a U.S. terminal, I can readily agree with your point that that is not an involvement of a U.S. person.

But where a U.S. person is targeted abroad or when it is determined that a U.S. person is being under surveillance from a foreign call, why not require a statement of probable cause and approval of a warrant by the Foreign Intelligence Surveillance Corps?

Mr. WAINSTEIN. Yes, sir. Good questions. Two separate questions. In terms of the question of whether we should have to go to the FISA Court to make a probable cause showing before we surveille a U.S. person outside the United States, that arose in the context of an amendment that was attached to the Senate Intelligence bill that was reported.

Senator SPECTER. The Wyden amendment.

Mr. WAINSTEIN. Right, the Wyden amendment. And that has been an area of much debate back and forth. As you know, under traditional procedures since 1981, FISA did not require that we get a—in the statute itself in 1978, it did not require that we get a court order for a U.S. person overseas because of that person's U.S. person status.

Instead, what we had is an executive order that was passed in 1981 that required that every time the government wants to surveille a U.S. person overseas, the Attorney General, himself or herself, personally, has to make a finding of probable cause that that U.S. person is an agent of a foreign power.

That was challenged at least once in court and has been upheld as reasonable under the Fourth Amendment. It has worked quite well. We have minimization procedures that limit the dissemination, use and retention of U.S. person information that we get from those surveillances, and our argument is that mechanism has protected American civil liberties quite well.

There are downsides to imposing that, as well, operational downsides. For one, you're taking the FISA court and, for the very first time, putting the FISA court into surveillances targeted outside the United States.

The statute itself will be saying, for a person who's outside the U.S., you still have to go to the FISA court, which is a new extension of FISA court jurisdiction.

Operationally, it would also potentially bring the FISA court into the realm of having to deal with foreign laws, for instance, laws that might be in effect in the foreign countries where we want to do the surveillance.

So there are some complicated operational matters, some which I think are better left to be discussed in a classified setting, that I think are implicated by requiring that all overseas surveillances against U.S. persons have to go the FISA court.

Senator SPECTER. Thank you, Mr. Wainstein. Thank you, Mr. Chairman.

Chairman LEAHY. Thank you, Senator Specter.

Senator Feinstein.

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

Mr. Wainstein, welcome.

Mr. WAINSTEIN. Good morning.

Senator FEINSTEIN. I think there are two big issues in this bill. One is the immunity provision. The other, in my view, is the exclusivity provision of the bill.

Senators Snowe, Hagel, and I filed some additional views, which I would like to urge you to read. And what we stated is our very strong belief that we believe FISA should be the only legal way of acquiring communications of people inside the United States and U.S. persons outside of the United States in certain circumstances for foreign intelligence purposes, and we go ahead and elaborate on it.

Now, the language in this bill was an Intelligence Committee compromise in the sense it was the best, certainly, I could do at the time. I am not at all satisfied with it, because it is not comprehensive and it does provide some loopholes, and I think those loopholes, candidly, are unacceptable.

It is my belief that the administration exceeded its authority in moving ahead with the terrorist surveillance program, and it is also my belief that we have ample history going back that this has happened before in the same way that led to the foundation of the bill before us, and, of course, that was the Shamrock case in the 1970s.

Somehow we don't learn from our mistakes. I am very concerned about the use of Presidential authority in this area. The President has claimed the AUMF. I'm here to say that when the AUMF was passed, there was no congressional intent that it be used for this purpose. That was not discussed.

I was present at many of the meetings. There was no discussion on allowing the AUMF to be allowed for Presidential authority in this area. And I believe the initial part of the terrorist surveillance program was, in fact, illegal.

So I want to strengthen the exclusivity provisions to prevent any loopholes and to see that it is clear for the future. That's the first point.

The second point is on the subject of immunity, and this is where it becomes extraordinarily difficult for me, with my belief that the administration proceeded illegally. Nonetheless, I've read the letters sent to the companies.

I'm aware of the fact that assurances were made to the companies by the executive branch of government. Those assurances may well have been wrong, but, nonetheless, these were the assurances that the companies were given. This happened 3 weeks after 9/11. I understand the tenor within the country.

The letter sent to us, dated October 29 and signed by Attorney General Ashcroft, James Comey, Jack Goldsmith and Patrick Philbin, makes this comment: "When corporations are asked to assist the intelligence community based on a program authorized by the President himself and based on assurance that the program has been determined to be lawful at the highest levels of the executive branch, they should be able to rely on those representations and accept the determinations of the government as to the legality of their actions."

I happen to agree with that. Then it goes on to say, "The common law has long recognized immunity for private citizens who respond to a call for assistance from a public officer in the course of his duty."

But the question arises as to whether the situation can't be better handled, because FISA has both a criminal and a civil prohibition in it, and, therefore, I wonder how the administration would feel about the capping of damages at a low level.

And the problem with indemnification is, we score this bill at $20–$30 billion, and that becomes a problem, I think, when you say the taxpayers should pick this up. This isn't a mistake made by the taxpayers. It's a mistake, I believe, made by the administration.

So the question comes, what sense does it make to proceed with an indemnification and a cap at a low level?

Mr. WAINSTEIN. Thank you, Senator Feinstein. I'll take those in reverse order.

I sort of answered that question, to some extent, to, I believe, Senator Specter, in terms of whether indemnification addresses all our concerns.

Obviously, if there is a cap, then it does address the concern that the taxpayer might get hit with high damages. But all those other concerns would still obtain. We'll still go through litigation, to the extent that state secrets doesn't short-circuit it. There's still the risk that classified, sensitive information will be disclosed.

The providers themselves will go through potential reputational damage. They'll go through the difficulty of litigation, depositions, discovery and the like, all for having done something which, as you said, was based on the assurances from the highest levels of the government of the legality of that program and they did so out of the patriotic sense that they wanted to help protect the country against a second wave of attacks after 9/11.

So all those other issues, I think, are still there, even if you do cap the damages.

As to your first question about the terrorist surveillance program and the—

Senator FEINSTEIN. Exclusivity.

Mr. WAINSTEIN [continuing.]—Question of the exclusivity clause, I know there is an exclusivity clause that's in the Senate Intelligence bill. I think it makes the point quite clearly.

As I said earlier, I believe that the nice thing about that legislation and this process is that we seem to be moving toward a point where we are all on the same page, that there is not going to be any need for the executive branch to go beyond what FISA has required.

Senator FEINSTEIN. That's not what this language does. It's specifically crafted in order to get it in that would allow a loophole or more than one loophole.

Mr. WAINSTEIN. Well, it says that it is the exclusive means, that the President, if he signs this legislation, is agreeing to that.

We have operated in accordance with that since January of this year. As you know, we went to the FISA Court. We took the terrorist surveillance program and brought it under FISA court orders on January 10 or 17 of this year.

So the terrorist surveillance program is no more. It is under FISA court order, and I think that's an important thing for us to have done prior to the time that we came to Congress about this legislation because it shows that we are operating within FISA, even within the constraints of old FISA.

And I believe that you will then see that if we have a scheme which we can use much more easily to protect the nation, there's going to be even less need for this President or future Presidents to go outside of FISA.

And keep in mind, nobody can bind future Presidents as to what the constitutional duty is one way or the other.

Senator FEINSTEIN. My time is up and I want to be respectful of the time.

I disagree with you about the exclusivity. I think this is a subject for a classified session and I think that the administration should be very candid with us as to what is in exclusivity and what is out of exclusivity, and I'll leave it at that.

Mr. WAINSTEIN. If I may, Senator Feinstein. I appreciate that and we would be very happy to talk to you in a classified setting, because there are some operational concerns that we only could air out in a classified setting about certain exclusivity clauses that have been proposed.

Senator FEINSTEIN. All right. Thank you.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

Normally, it would be Senator Hatch, but he's not here.

Senator Kyl.

Senator KYL. Thank you, Mr. Chairman.

I just want to start with—there was a comment made earlier about the Department of Justice being dysfunctional, and I would dispute that.

It is true, I think, that it's in desperate need of leadership, which of course could be cured if the Attorney General nominee were confirmed, but I think there are a lot of good men and women at the Department who are doing their job under difficult circumstances, and we should recognize that.

My first question, Mr. Wainstein, concerns the legal authority for the foreign surveillance program and it is whether you know of any case—the only case of which I am aware that has spoken to the issue, and it's dicta, it's not a holding, but the case has never been squarely presented as far as I know, is a FISA case in 2002 titled "In Re: Sealed Cases."

And this is the pronouncement of the court in that circumstance: "The Fourth Circuit, in the Truong case, as did all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power."

Now, are you aware of that case?

Mr. WAINSTEIN. Yes, sir.

Senator KYL. Did I characterize it accurately, in your view?

Mr. WAINSTEIN. Yes, Senator. That's my understanding of the case.

Senator KYL. Do you know of any other case in which a court has spoken to this question, which goes, of course, to Senator Feinstein's point about exclusivity?

Mr. WAINSTEIN. No. Actually, as you quoted from that case, the courts that have addressed this issue have determined that the President does have that authority and they've been consistent in that.

Senator KYL. Furthermore, in your testimony, on page four, you talk about the historic surveillance that we have conducted and the history of FISA, establishing a judicial review regime, but not for all of our foreign surveillance.

You say only for certain of those that most substantially implicated the privacy interests of the people of the United States, which I think is accurate, and you point out that it was not intended to apply to all overseas surveillance.

And you went on to note that the House report at the time, the House Permanent Select Committee on Intelligence report, 1978—I would add that that was under Democratic control—confirmed that this was the case and, quoting that report, which explained that "The committee has 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 surveillances," making the point that we have had for decades overseas surveillance which has not required going to through any court to obtain a warrant.

Is that correct?

Mr. WAINSTEIN. Yes, under the wording of the statute—and, of course, the problem is that—and what we're trying to remedy here is the problem that has taken us away from the original design of FISA, which is as you just described it, and, that is, as I think we also explain in the statement, a function of the evolution of the technology since 1978.

And the fact is the original FISA was designed—it was actually—the terminology of the statute was based on the types of technology that were going to be intercepted, wire or radio, and that has changed dramatically, bringing in all these communications within FISA that weren't intended to be within FISA to begin with, primarily the ones outside the United States.

Senator KYL. Exactly. Now, there's also been some language thrown, and I think we should be a little careful of throwing around words like "amnesty." Amnesty obviously refers to a situation in which a crime was committed and that crime is going to be forgiven.

Is that your understanding of the word "amnesty?"

Mr. WAINSTEIN. More or less.

Senator KYL. Do you know any allegation, or at least any fair allegation, that any of these telecom companies committed a crime for which they might need some kind of amnesty?

Mr. WAINSTEIN. No, Senator Kyl, quite the opposite. My sense is they were operating out of a sense of patriotic duty.

Senator KYL. Well, that's my sense, too. And I wanted to quote something from Judge Cardozo, because I think it applies here, in a case called *Babington* v. *Yellow Taxi Company*.

He said, "The rule that private citizens, acting in good faith to assist law enforcement, are immune from suit ensures that," and this is the case, the words of Justice Cardozo, "the citizenry may be called upon to enforce the justice of the state, not faintly and with lagging steps, but honestly and bravely and with whatever implements and facilities are convenient and at hand."

Now, it seems to me that that captures the obligation and responsibility that we expect of citizens who are in a unique position to assist our government in a situation like this and that we should be bending over backward to ensure that they are protected in that assistance for the national good.

The differences between the suggestion of indemnification and providing immunity, it seemed to me, are worth exploring, and some of my colleagues have raised some of those questions with you.

You have indicated that there are a variety of reasons why it would still be difficult, if there is indemnification, to protect American secrets and to protect the companies from all of the exigencies of litigation that would occur prior to the time that the suit were brought to a conclusion.

If the State Secrets Doctrine were not successful, would these suits necessarily be brought to conclusion any time before a final judgment for which then the government might be responsible?

Mr. WAINSTEIN. It would go forward after the State Secrets Doctrine was—

Senator KYL. So if that defense is not successful, they go through the case. They have to testify. They have to bear the expenses. They may be indemnified, but in addition to the possibility that the secrets would be revealed, there would be all of the difficulty of going through this litigation, notwithstanding the fact that, at the end of the day, they would be reimbursed for their trouble.

Mr. WAINSTEIN. Absolutely. And I think not only is it unfair to them and would they suffer reputational damage and cost and expense and have to overcome the difficulties of litigation, but, also, as I said earlier, we work on a cooperative basis with these companies and we can't do it—we cannot do communications intelligence without them. Unless we nationalize the communications industry, we have to go through them and we have to rely on their cooperation.

And sort of to go back to what you quoted from Justice Cardozo, just like the police officer on the street, I was trying to think of an analogy. If a cab driver drives by a bank and a police officer comes running out, bells are going off, alarms going, he says, "Go after that speeding car," and jumps in the front seat, we don't want the cab driver to sit there and say, "Well, let's think through all the different possibilities. Maybe you're not really a police officer. Maybe that's not the bank robber. Maybe you're actually in a fight with somebody out of a bar next door to that bank," all these other things.

You want a person or a company who perceives apparent authority on the part of law enforcement to act. And if these companies are subject to liability, they're going to have a disincentive to act in the future and they're going to challenge any requests that we

make to them, litigate to the nth degree, because they think that that's the way they're protecting the rights of their shareholders.

We don't want to be in that situation because that will really detrimentally impact our operations.

Senator KYL. Let me just ask you one final question regarding the so-called Wyden amendment.

It is not limited to citizens, is it? In other words, it appears to cover "U.S. persons," which would also include U.S. green card holders, which, therefore, could mean any number of people who may live abroad, but have a U.S. green card. Is that correct?

Mr. WAINSTEIN. Yes, sir.

Chairman LEAHY. I just want to make sure I fully understand, whether we call it amnesty, immunity or indemnification.

Prior to this being made public in the press, apparently from somebody within the administration, there was only this Presidential directive. After it was made public, the administration then went to the FISA court. Is that correct?

Mr. WAINSTEIN. Mr. Chairman, we went to the FISA court—well, we obtained FISA court authority for the TSP, the surveillances that were done under the TSP in January of this year. That was after a long process.

Chairman LEAHY. After it became public. And there's no question in your mind, if a telephone company has a court order, that clears them. They're totally—there's no liability on the part of a telephone company response or anybody responds, a bank responds to a court order to give over a bank record, a telephone company responds to a court order to give telephone records.

No suits can go against them because they responded to that court order. Is that correct?

Mr. WAINSTEIN. Yes, sir, that's a defense. If I could just clarify one thing. I believe we've said publicly that we were actually engaged in the process leading to the FISA court orders prior to the public disclosure of the program. I believe that we've said that.

I just wanted to clarify that as to when we went to the FISA court. I wasn't there at the time.

Chairman LEAHY. I actually have the chronology in mind, but I heard that in a classified session so I'm being very careful not to go into it.

Mr. WAINSTEIN. Thank you, sir.

Chairman LEAHY. Senator Feingold was one of our crossover members from Judiciary and Intelligence.

Senator FEINGOLD. Thank you, Mr. Chairman.

First, Mr. Chairman, the role of this committee, as you well know, is so important on this issue and I'm so glad you're having this hearing.

I am a member of the Intelligence Committee, as well as the Judiciary Committee. I've been following this issue for almost 2 years, since the day it was revealed in the New York Times, and shortly thereafter I became a member of the Intelligence Committee.

After a bit of a struggle, I had the opportunity to be read into the program. My staff has also been read into the program.

I want this committee to know my view that the product of the Intelligence Committee doesn't do the job. There can be as much bipartisanship and collegiality as you can possibly have, but the

bill still is not adequate and the mere fact that it's bipartisan, obviously, doesn't make it constitutional.

This process reminds me what happened with the Patriot Act and the subsequent renewal of the Patriot Act. We had the rush to judgment in the beginning, that was somewhat understandable given the timeframe. But then, in my view, we failed to correct the Patriot Act in significant areas, and three Federal courts have struck down important provisions of the Patriot Act.

Mr. Chairman, we're heading in the same direction here if this committee does not do its job and fix the errors that were made in the Intelligence Committee.

Having said that, I want to get back into this issue of executive power that both Senator Feinstein and Senator Kyl have talked about.

Mr. Wainstein, right now, does the President have the authority to authorize surveillance beyond what is permitted by FISA, as amended by the Protect America Act?

Mr. WAINSTEIN. Senator Feingold, that's obviously a question with constitutional implications. What is the constitutional allocation of authority to the executive branch to defend and protect the country against external threats?

And the argument that I think was laid out in the white paper that was issued by the Department of Justice back in the aftermath of the disclosure of the TSP, that the President did have certain inherent constitutional authority to conduct electronic surveillance or communications surveillance to protect the nation.

As I said earlier, though, I think that this legislation obviates the need to actually engage in that issue.

Senator FEINGOLD. I know that's the exchange you had with Senator Feinstein. So let me just put it on the record.

If the bill passed by the Intelligence Committee became law, would the President have authority to authorize surveillance beyond what would be permitted by that bill?

Mr. WAINSTEIN. Once again, Senator Feingold, it's not for me to say, to either stake a claim to or to give up constitutional authority to the President. It's not even this President's—

Senator FEINGOLD. What is your view?

Mr. WAINSTEIN. I'd have to actually go back and take a good hard look at all the constitutional underpinnings of that issue. But I've read the positions on both sides. There are good arguments both ways.

But there's clearly authority for the executive branch to do warrantless surveillance and, as Senator Kyl has said, the courts that have addressed this issue have uniformly found that the President has that authority, including the 2002 opinion of the FISA Court of Review.

So I think the law to date is pretty clear on that issue.

Senator FEINGOLD. I take the opposite view. I think it's clear under Justice Jackson's test, with regard to when Congress has spoken, that the opposite conclusion is warranted. But I think we're going to have to get a new President in order to have a different view that is not so expansive and, I think, dangerous with regard to executive power.

In the Intelligence Committee bill, the government is required to inform the FISA court about its minimization procedures. First, the government's minimization procedures are provided to the court for approval after they've gone into effect, and, second, the government has to provide the court with its own assessment of its compliance with those procedures.

But under the bill, what can the court do, Mr. Wainstein, if it believes the government is not complying with its minimization procedures, which the administration argues provide such great protection for U.S. persons?

Mr. WAINSTEIN. Well, Senator Feingold, you're focusing on the question of what it is we have to do with our minimization procedures vis-á-vis the FISA court.

The FISA court, under this bill, will review the minimization procedures, make sure they're reasonable, make sure they satisfy the statutory requirement for minimization procedures.

It does not have them conducting ongoing compliance reviews of those minimization procedures and I think there are reasons for that. In the original FISA context, they do. So we have to get individual orders when we get FISAs, under the original FISA, for people in the United States and there are minimization procedures that apply to that particular surveillance, and the FISA Court does review compliance.

We provided—

Senator FEINGOLD. This reminds me almost of a right without a remedy. The court gets to review it, but has no power to do anything about it. Is that what you're saying?

Mr. WAINSTEIN. Well, the problem here is that, as you know, this bill allows for programmatic sort of surveillances by category and this would be a much more comprehensive compliance review by the FISA court, making them much more operational than they ever have been in the past.

Senator FEINGOLD. Again, this involves a court that would have the opportunity to review these minimization procedures, and I hope my colleagues are hearing this, with no ability to do anything about it, no ability to say to the administration, "You screwed up and you've got to change this."

This is in this intelligence bill that's being labeled as an adequate control over the executive.

Mr. WAINSTEIN. If I may, Senator Feingold.

Senator FEINGOLD. Yes.

Mr. WAINSTEIN. I see your point there and I think it is worth mentioning, however, that there are any number of oversight mechanisms in this bill and we're not opposing these. We're not opposing—we've got a couple operational concerns with one or two, just in terms of the feasibility, but by and large, we're not.

And, in fact, if you look, and I mentioned this earlier, if you look at the way we've conducted operations under the Protect America Act, we have, as I said, imposed a lot of oversight on ourselves and tried to be as completely transparent as we can with Congress, so that Congress, if it sees a flaw, can do something about it.

And we're continuing that approach here, because we understand that that's the only we can retain these—

Senator FEINGOLD. I appreciate the answer and hope my colleagues heard it. They have imposed these rules on themselves. We do not have internal rules. We do not have the court having the ability to deal with these problems.

In September, I asked DNI McConnell whether the bulk collection of all communications originating overseas, including communications with people in the U.S., is authorized by the PAA. He responded, "It would be authorized if it were physically possible to do it."

Would this same wide-sweeping type of bulk collection of all communications originating overseas, including those with people in the U.S., be prohibited in any way by the Senate Intelligence Committee bill?

Mr. WAINSTEIN. Well, if you're referring to the idea that we would just have a vacuum cleaner and soak up all overseas communications, one problem there, of course, is that we can only do this if there's a foreign intelligence purpose to it and we're getting foreign intelligence information, and, presumably, a vacuum cleaner approach like that would not be selecting only those communications that have foreign intelligence—

Senator FEINGOLD. Would you have any objection to making it clear that this type of extremely broad bulk collection is not authorized by the bill? Would you be willing to support language to that effect?

Mr. WAINSTEIN. We'd have to take a look at the language, obviously, to make sure it doesn't have unintended consequences, limiting us in ways that we don't intend. But we'd be happy to take a look at it.

Senator FEINGOLD. My time is up, but I do hope you'll consider that. Thank you.

Mr. WAINSTEIN. Thank you, sir.

Chairman LEAHY. Senator Sessions.

Senator SESSIONS. Mr. Wainstein—and I would just say to Senator Feingold, you have been direct and honest about your approach to it. The matter was considered in the Intelligence Committee, but by a 13–2 vote, they concluded otherwise.

Congress does have oversight responsibility. It is our responsibility to ask about these programs. We have the ability, which we have done, to have the top officials that run these programs testify before us and explain them in great detail, ask questions, and we've had the opportunity to cut off funding or prohibit these programs from going forward.

I would say, when we passed the Protect America Act to extend this program, what this Congress did, was it heard the complaints, it had an in-depth review of what the administration was doing.

We found the critical need for the program. We studied the constitutional objections that had been raised and we concluded that it was legitimate, and we affirmed it and we approved it.

Isn't that fundamentally what's happened, Mr. Wainstein?

Mr. WAINSTEIN. As far as I can tell you, yes, sir.

Senator SESSIONS. All right. So we have approved this program, and we approved it because it was the right thing.

I just had a visit to the National Security Agency last week and went into some detail and I came away even more convinced than

from the previous briefings I had had just how critical this program is for our national security.

Mr. Wainstein, based on your observation and research, do you consider this to be a critical program for our national security and do you believe that we absolutely, for the security of the American people, need to continue it or something like it?

Mr. WAINSTEIN. Absolutely, Senator Sessions. When we talk about the program, the interception of signals or communications intelligence is absolutely critical, and that is how we learn what our adversaries are planning to do. We capture their communications. We capture their conversations.

And while we'd be happy to talk to you in a classified setting about actual case studies or case anecdotes to explain how we've gotten critical information with the Protect America Act, I can't talk about it here publicly, but it is an absolutely critical piece of our operations.

And if you talk to the NSA and you see how quickly we are able to implement the Protect America Act authority, they will tell you how quickly those gaps that the DNI was talking about prior to August 5, how those gaps closed just like that.

Senator SESSIONS. In fact, that's exactly what I heard last week. And I have to emphasize to my colleagues, if you talk to the people at NSA, you know they are very careful about what they do. They self-restrict themselves. They know that people can complain if they overreach.

They are not overreaching, I don't believe, and I'm proud of what they're doing. It's saving lives, not just in the United States, but it is saving lives of those men and women in our military service that we have committed to harm's way, who are at risk this very moment in places like Iraq and Afghanistan and other places, and it's helping preserve their safety and their lives, and it's constitutional, and we've already said that. So, I think we should continue with this program.

So now we're reduced, I think, to an argument over whether we ought to allow people to sue the telephone or the communications companies that have cooperated at the request of the government to protect this country after 9/11.

And I don't think it's a right phrase, as I think as our Chairman said, to say we are letting them off the hook. They shouldn't be on the hook. They did what their country asked them to do. They were told in writing that it was legal, were they not, what they were doing?

Mr. WAINSTEIN. Yes, sir. They were given assurances, the same assurances that—

Senator SESSIONS. And I just don't think they ought to be hauled into court, and the people filing this lawsuit using it as a vehicle to discover everything they can discover about some of the most top secret programs this country has. And that does happen in these cases, does it not?

Mr. WAINSTEIN. Absolutely. This is the most confidential and classified sensitive information that we have in our national security apparatus, and those are the details that get disclosed during that litigation.

Senator SESSIONS. And I think one of our colleagues earlier said, well, this may be the only way that—the only outside review of this program.

Well, we're the ones that are supposed to review this program, are we not, as representatives of the American people? Would you agree with that?

Mr. WAINSTEIN. Yes, sir. And there's quite a bit of oversight from Congress. And, as I mentioned earlier, there are a number of different investigations being carried on right now by inspectors general and offices of professional responsibility and the like, looking into the appropriateness of the terrorist surveillance program.

Senator SESSIONS. And some private lawsuit out here against companies for millions of dollars, filed by lawyers who could be lawyers associated with groups associated with terrorism, is not the way to give oversight to a program like this, I don't think.

Would you agree with that?

Mr. WAINSTEIN. I go to the fundamental point, Senator, that these companies were operating at our request, upon our assurance. And so if people have a problem with it, if there's fault there, they should direct their concerns to the government. The government should be the ones who are called to answer and not the companies that were acting out of patriotic duty.

Senator SESSIONS. Well, I'm also of the belief that—I believe someone stated that the telecom companies would believe that indemnification is sufficient.

My impression is they do not, because they're still subject to the lawsuits. Do you have any information about that?

Mr. WAINSTEIN. I don't have any direct information as to what their position is, except I know that they much prefer immunity, and that's certainly our position.

I believe, though, that they would see all the same problems with indemnification that I have listed for your colleagues.

Senator SESSIONS. Well, I am certain they would. It only makes common sense. And I believe, in fact, they don't think that's the best way, that the indemnification approach is best.

Mr. Chairman, I just offer, for the record, an op-ed in today's *Wall Street Journal*, written by Benjamin Civiletti, a former Attorney General under former President Jimmy Carter, Dick Thornburgh, a former Attorney General under former President Bush, and William Webster, former head of the FBI and the CIA, that testify to the importance of this legislation and they strongly support the view that these companies that have cooperated should be protected from lawsuits.

They say the companies "deserve targeted protection from these suits" and point out that dragging phone companies through protracted litigation would not only be unfair, but it would deter other companies and private citizens from responding in terrorist emergencies whenever there may be an uncertainty or legal risk.

I would offer that for the record.

Chairman LEAHY. Thank you. Without objection, it will be part of the record.

[The article appears as a submission for the record.]

Chairman LEAHY. I just want to make sure I fully understand, from your testimony, following on a question by Senator Sessions.

Has there been any suggestion by any Member of Congress, of either party, that we should not be doing electronic surveillance of people who may pose a threat to the United States?

Mr. WAINSTEIN. Not that I have heard, Chairman Leahy. In fact, I think what we're seeing now—not in the course of this debate. What we're seeing now is, I think, a fairly good consensus in the American people and in Congress that we need the tools to do it and we should not have to get a court order if we're targeting persons outside the United States, with the exception of—

Chairman LEAHY. Because I just don't want—and I'm sure the Senator from Alabama did not mean to leave the wrong impression here, but I certainly don't want any impression being here that—I've sat through hundreds of hours of briefings and closed sessions and open sessions on this. I have yet to hear any Senator or any House member, of either party, say they feel that we should not be surveilling people who have positions inimical the best interest of the United States.

Senator SESSIONS. Mr. Chairman, just to respond to that, I would say that this administration has been under severe attack for programs, including this program, severe political attack, often from outside, sometimes within Congress, and by passing the Protect America Act and by the vote of the Intelligence Committee, this Congress has said they are doing legitimate work and we affirm their work.

Chairman LEAHY. I think this Congress, many people were concerned that the White House was not following the law and wanted them to follow the law.

I was concerned when the President of the United States said FISA was a law that had been basically unchanged since the 1970's. Of course, it has been changed 30-some-odd times since then.

And I think that if there had been criticism, it's simply been that the United States, which stands for the rule of law, ought to follow the law.

Mr. WAINSTEIN. If I may, Mr. Chairman.

Senator SESSIONS. Well, I think we concluded that the President is following the law. That's why we've affirmed the program as it is presently being executed.

Chairman LEAHY. Mr. Wainstein.

Mr. WAINSTEIN. I just want to say that my answers related to—when we were talking about the program, the idea of doing foreign intelligence surveillance against persons overseas without going to the FISA court first and that's been the area of disagreement, at least that's what has been hashed out in debates over the last month or two.

Chairman LEAHY. Senator Cardin.

Senator CARDIN. Thank you, Mr. Chairman, and I particularly thank you for clarifying the record, because every Member of Congress wants to make sure that we gather the information we need and we want to make sure it's done in a way that's consistent with the civil liberties of the people in this country and the constitutional protection.

Quite frankly, I think that by complying with that, the collection of information will be more valuable to our national security interests. So it's in our interest to do it for many reasons.

I want to question you on a couple points that you mentioned. You first talked about your concern about the sunset that's included in the Senate bill and the House bill; the Senate bill has a 6-year sunset, the House bill has a 2-year sunset.

And you then talk about your cooperation with Congress, making a lot information available to us. I somewhat question whether we would have gotten the same level of interest by the administration in supplying information to our committees if there were no sunset included in the legislation, if we had a permanent extension of the law.

And, secondly, I want you to comment on the fact, 6 years from now, can you anticipate what technology is going to be? It seems to me it's a good idea for us to be required to review this statute, not only because of its sensitivity on the civil liberties, but also on the fact that technology changes very quickly and we need to make sure that we have this law reviewed on a regular basis.

So why isn't a sunset good?

Mr. WAINSTEIN. Thank you, Senator. That's a good question. I've actually spoken quite a bit about the appropriateness or inappropriateness of sunsets.

I'm not reflexively resistant to sunsets at all. I think they actually have a very important place, and I think they had an important place with the Protect America Act.

When Congress is in a position of dealing with an immediate need in legislating, without maybe feeling like it has the time to go through and check the record and deliberate and debate completely and look at all the angles, then it makes sense to have a sunset, just as we had in the Patriot Act, which was passed, I believe, 6 weeks to the day after 9/11, with a huge, large raft of new provisions.

Sunsets were put in place there to make sure that Congress then had the time to go back and reevaluate things and make sure they didn't miss anything and see how these tools are being implemented.

Same thing with the Protect America Act. You all responded to the need in the summer. You put a sunset in place, and I think we're going through a very healthy process right here. I think this is great.

Senator CARDIN. Some of us think we need to continue that process.

Mr. WAINSTEIN. And I think that's why we're not resisting the oversight—the very ample oversight—and congressional reporting requirements in this bill.

My feeling, however, is that once you've had that debate, go ahead and legislate. You don't need to put a sunset. Congress can always re-legislate in FISA, and has many times over the years.

Senator CARDIN. It's sometimes more difficult than it may seem, and when we're required to act, we act.

Mr. WAINSTEIN. I understand that. But you've got to keep in mind there's a downside to that, too, because whenever you confer authorities, legal authorities on law enforcement and the intel-

ligence community, that starts a process, which is a very in-depth process, of agencies drafting policies, putting procedures in place, training people, and then when you have to shift gears—

Senator CARDIN. I think Congress has the responsibility and I think it's helpful to us to have the sunsets in law.

Let me go to the U.S. Americans who are targeted overseas and the amendment that was put on that you have concerns about.

I, quite frankly, don't understand the concern here. It's my understanding there have been published reports of how few people actually fall into this category, and it seems to me we always want to balance the rights of individuals versus the inconvenience or difficulty in complying with the probable cause standards.

It seems to me, here, this is an easy one, that going and getting a warrant should be the standard practice.

Mr. WAINSTEIN. Yes, Senator. And we've heard that view from a number of your colleagues.

I guess, keep in mind, as I explained earlier, there is a process in place by which we—the Attorney General personally made a probable cause finding for people overseas.

The FISA court did, on occasion, provide FISA court authority for U.S. persons overseas, because of the way the technology evolved since 1978.

Senator CARDIN. But I am correct, there's just a few number that fall into that category.

Mr. WAINSTEIN. I can't go into the classified—

Senator CARDIN. I thought there was some information that had been released on that.

Mr. WAINSTEIN. I think there's been some public discussion about it, but I'll tell you, as I sit here right now, I'm not sure what I'm authorized to say or not say.

Senator CARDIN. The director of National Intelligence evidently has said it and, it seems to me, if he's said it—

Mr. WAINSTEIN. Right. Well, I think he has declassifying authority that maybe I don't have.

Senator CARDIN. Okay. Well, his number, I believe, was the mid-50's, 55 or 56 people that actually were subject to this, which is certainly not a huge burden to get that information. And I think that's where you lose some credibility when you have an issue that can be easily resolved and, yet, you try to get the authority to avoid what seems to be core to American values, and that is having cause to get a warrant against an American.

I want to get to the immunity. I have 2 minutes left, and this is a difficult subject and this is one that I think many of us are wrestling to try to get right.

You used the Good Samaritan analogy, where someone is on the scene of an accident and needs to respond quickly, and I can understand that being used on September 11.

This program has been reauthorized for 5 years or 6 years. It seems to me that this is difficult to use that analogy when the telephone companies or servicers had plenty of chance to review the circumstances and make independent judgment.

And I guess my point to you is, do you think the service providers have any responsibility to the privacy of their customers to

make an independent judgment as to whether this information was properly requested?

Mr. WAINSTEIN. If I could just very briefly discuss the U.S. person overseas issue, just because I don't want to leave one thing hanging.

I understand your concern. There are operational concerns that we have, especially about one aspect of that provision, that we'll need to discuss in classified session.

Senator CARDIN. You mentioned that earlier.

Mr. WAINSTEIN. There are also some issues—there's no emergency provision there. Also, keep in mind that in terms of what is sort of the standard American approach, that requirement is not in place on the criminal side, on the criminal law enforcement side, either, so there is some question there about what is sort of more traditional or not.

But I would like to followup with that, with you or anybody else, in a classified setting.

Senator CARDIN. Certainly.

Mr. WAINSTEIN. In terms of the obligation of the carriers, there are delineated legal obligations that carriers have.

Senator CARDIN. They have pretty big attorney staffs, legal staff. These are not unsophisticated companies.

Mr. WAINSTEIN. Yes. But I don't know if you actually saw the documents yesterday.

Senator CARDIN. I have seen them.

Mr. WAINSTEIN. The letters.

Senator CARDIN. Yes, I have.

Mr. WAINSTEIN. Some of the letters that were sent to the carriers explaining—

Senator CARDIN. And I don't know. If this is an inappropriate question, I'm sure you'll mention that. It seems to me that if I were the lawyer for the service providers, I would have asked for indemnity.

These are sophisticated companies, so they can make independent judgments. I understand the concern on September 11, but this has been going on for many years. I find it hard to believe that large companies with big legal staffs never ask for more protection or more information.

Mr. WAINSTEIN. Well, I can say that as the bill out of the Senate Intelligence Committee reflects, there are certain common sense criteria you'd look at for them to have a suitable reliance on the government in going forward and assisting the government.

If you look at those documents—I can't get into the classified nature of them—you'll see that those assurances are there. I think they operated on a good faith basis, and I don't know that we want the legal staffs of all these communications providers putting us through the paces and litigating everything.

As you know, under this legislation, as under the Protect America Act, these carriers can challenge every one of the directives we give them and really slow down our operations.

So I don't know that we want to encourage that. In fact, I think we want to not encourage it by alleviating any possibility of retroactive liability.

Senator CARDIN. Thank you, Madam Chair.

Senator FEINSTEIN [presiding]. Thank you, Senator.

Senator Cornyn is next up.

Senator CORNYN. Thank you, Madam Chairman.

Mr. Wainstein, the Protect America Act sunsets in February. Is that correct?

Mr. WAINSTEIN. I believe it's February 1st, sir.

Senator CORNYN. And that's the law that Congress passed this Congress that said if it's two terrorists talking to each other overseas, that we don't need to get a warrant to intercept that information. Correct?

Mr. WAINSTEIN. If we're targeting our surveillance at a person overseas, we don't have to go to the FISA court before doing that.

Senator CORNYN. And you're asking here today for a permanent extension of that law which Congress has already passed. Correct?

Mr. WAINSTEIN. Yes, sir. Basically to bring it back in line with what was the original intent of FISA back in 1978.

Senator CORNYN. Let me take this down to a particular scenario or set of facts that I think will help us understand what a burden the need for a warrant can be when it comes to communications between terrorists overseas. On October the 16th, the New York Post reported a story involving some soldiers who were in Iraq and were killed by Al Qaeda operatives, four killed and three were then kidnapped, including Alex Jiminez from Queens, and later, as a result of the search to find the three kidnapped soldiers, one of my constituents, Ryan Collins, 20 years old, of Vernon, Texas, lost his life.

But the time line here I think is significant because, at 10 on May the 15th, after these three soldiers were kidnapped, U.S. officials came across leads that show need to access to signals communications, and the NSA, at 10:52, 52 minutes later, notified the Department of Justice that, under existing FISA law, a warrant was needed to eavesdrop because of communications passed through United States infrastructure, even though it was communications overseas between two foreign nationals.

It then took till 12:53 p.m. for lawyers and intelligence officials to begin to work to confirm the probable cause necessary to identify the kidnappers as foreign insurgents, and therefore a legitimate target of American surveillance. Then almost 5 hours later, at 5:15 p.m., the lawyers were able to file the paperwork necessary to request the emergency surveillance.

Finally, at 7:18 p.m. that night, almost 10 hours later, the Attorney General of the United States approved the emergency surveillance based upon the belief that the FISA court would grant the warrant retroactively within 1 week.

So 9 hours and 38 minutes after three American soldiers were kidnapped, and after it became apparent that there was signals intelligence that might help identify who their kidnappers were and where these American soldiers were located, it took almost 10 hours to get the necessarily paperwork done by the lawyers at the Department of Justice in order to get the approval for the kind of surveillance that was required.

Is that the kind of impediment or barriers to signals intelligence surveillance that you are asking that the Congress avoid and eliminate so we can hopefully save American lives?

Mr. WAINSTEIN. Absolutely, Senator Cornyn. That particular incident—obviously it's classified. There is only so much I can say about it—it was a bit unique in the sense that there were some very novel issues of law there. However, even if you take it out of that context, so that I don't step in classified matters, into any emergency authorization context.

There is a provision that allows us to have the Attorney General, and now delegated to me, authorize surveillance on an emergency basis. Within 3 days, however, we have to go to the FISA court with a big package of materials and persuade the FISA court that there is probable cause that the person we are surveilling, who might well be outside the United States, is an agent of a foreign power. So we have to have all that probable cause before the Attorney General makes his determination.

It then has to be put into a package and satisfy the FISA court, or else there are consequences. That all takes resources. It also means that there are people who are legitimate targets overseas against whom we just cannot make probable cause that they are agents of a particular foreign power, and we cannot surveille them at all. So it is not only an impediment in terms of, it takes time, it takes resources, but it is precluding us—or it did preclude us—from surveilling legitimate targets overseas. It's much better now.

Senator CORNYN. Mr. Wainstein, you of course were talking about matters that are both public, and some classified which we are not going to talk about. But I just want to stress, the time line that I provided to you was in published news reports. I'm not asking you to confirm or deny that time line, but the report, according to the New York Post, was that it took 10 hours later.

And my constituents in Texas, the parents of this young corporal that lost his life searching for these three Americans soldiers who were kidnapped and whose discovery was delayed by 10 hours because of the red tape necessitated by the interpretation of the FISA law, I believe contributed to this young soldier's death.

Mr. WAINSTEIN. Absolutely. Absolutely, sir.

Senator CORNYN. And that's just simply unacceptable. I think it ought to be unacceptable to every American, when we are at war, to handcuff our American military and intelligence officials in this unacceptable way. Just, to me, it's a no-brainer. I just fail to understand why we need a "Guarantee Full Employment Act" for lawyers in order to fight a war.

Let me ask you, there's been some question about the retroactive immunity for the telecoms who have participated in the intelligence surveillance that you described earlier. There is some question whether we ought to cap damages, whether we ought to grant them some sort of reimbursement for their attorneys' fees, and other costs. But there are other tangible consequences associated with litigation which could be avoided.

I suggest to you that, during Judge Mukasey's testimony, we talked about the fact that during the 1993 trial involving the World Trade Center, where the trial of Omar Abdul Raman, the so-called Blind Sheik, who conspired to bomb the World Trade Center, that a list of 200 unindicted co-conspirators was disclosed to defense attorneys and later found its way into the hands of Osama bin Laden in the Sudan. Bin Laden was, of course, on the list. Does that high-

light one of the other risks attendant to litigation of this nature involving classified materials, sensitive classified information might find itself in the hands of our enemy?

Mr. WAINSTEIN. Yes. Absolutely. Now, of course that's a different context. The criminal context—we have discussed with Senator Specter the Classified Information Procedures Act, which helps us there. But still, even in that situation, you had disclosure of very sensitive information which was very detrimental to our effort against our enemies.

We are concerned that that is going to happen, even doubling, in this litigation. My understanding is, there are 40-some cases right now around the country. With all those cases running, we are gravely concerned that sources not be disclosed.

Senator CORNYN. Thank you very much.

Thank you, Madam Chairman.

Senator FEINSTEIN. Thank you, Senator.

Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Madam Chairman.

Just so it is clear what we are talking about, because I think everybody agrees that we don't want to handcuff our military and our security intelligence forces when they're out hunting foreign terrorists, the Protect America Act, as it passed by this Congress back in August, would allow no restriction or would establish no restriction on our intelligence agencies once a person was reasonably believed to be outside the United States. Correct?

Mr. WAINSTEIN. Yes, sir. There were various criteria that we had to satisfy before the DNI and the Attorney General could issue a certification. But the key finding was that the person we were targeting with surveillance was outside the United States.

Senator WHITEHOUSE. Was reasonably from outside the United States. And that category, "reasonably believed to be outside the United States", would include a family on vacation in the Caribbean, an American family, all citizens on vacation in the Caribbean, that category?

Mr. WAINSTEIN. If there was a foreign intelligence purpose to that surveillance, and if we demonstrated that that person or that family was an agent of a foreign power, yes.

Senator WHITEHOUSE. Where, under the Protect America Act, do you have to demonstrate that they are an agent of a foreign power?

Mr. WAINSTEIN. That's under the 12333.

Senator WHITEHOUSE. Exactly. It's not under the Protect America Act. There's nothing in the Protect America Act that would prevent the intelligence apparatus of the United States from surveilling American citizens on vacation in the Caribbean. Correct?

Mr. WAINSTEIN. One of the criteria is that there is a foreign intelligence purpose—this is in the statute—to that surveillance, and we have to meet that.

Senator WHITEHOUSE. That's rather broadly defined, isn't it?

Mr. WAINSTEIN. Well, I think—

Senator WHITEHOUSE. And there's no judicial review of that determination, is there?

Mr. WAINSTEIN. Well, there's a judicial review of the procedures by which we—

Senator WHITEHOUSE. But no judicial review of the determination that that family vacationing in the Caribbean is being surveilled for an intelligence purpose.

Mr. WAINSTEIN. Well, obviously the directives can be challenged. Congress set up a mechanism by which they can be challenged, so there is court review there. But in terms of going to the court—

Senator WHITEHOUSE. You must be reading a different statute than I am. I find no place in which a directive is required from a court authorizing a family vacationing in the Caribbean, or a businessman traveling to Canada, or somebody visiting their uncle in Ireland, from being surveilled by the United States. The FISA court is stripped of that jurisdiction by that statute, is it not?

Mr. WAINSTEIN. But the FISA court—right. The FISA court reviews the procedures by which we determine that those people outside the United States—

Senator WHITEHOUSE. Right. But they don't review the determination.

Mr. WAINSTEIN. They do not give us approval up front. That's the difference.

Senator WHITEHOUSE. Correct. I think that's an important point. I think what we're trying to get at here is, what is the best way to protect Americans when they happen to be traveling abroad? This is a different world now. People travel all the time, for all sorts of reasons. I don't think anybody in America believes that they give up their constitutional rights the instant that they cross the border.

You indicated that you thought that there was a difference between whether you are in the country or outside of the country in the criminal law as well. Has the Department of Justice, the United States Department of Justice, ever wire tapped an American citizen outside of the United States in a criminal investigation without a court order?

Mr. WAINSTEIN. I honestly don't know historically what the Department has authorized or not. What I'm talking about though, is that as you know—

Senator WHITEHOUSE. Are there any American citizens presently being surveilled by the Department of Justice outside of the United States without a court order in a criminal investigation?

Mr. WAINSTEIN. I wouldn't know. I'm going to be careful, because I just don't know, Senator. But the point I was—

Senator WHITEHOUSE. Will you take those two questions for the record, please?

Mr. WAINSTEIN. I would be happy to take them for the record and get back to you.

The point I was making earlier, sir, is that, as you know, in a criminal context there is not a warrant mechanism whereby a judge would issue a warrant for a search in Bangladesh or Buenos Aires, or whatever. My point is, just the fact that there isn't one on the national security side is not that striking because there's not such a mechanism on the law enforcement side either.

Senator WHITEHOUSE. It strikes me, though, as we're trying to resolve these difficult issues where we're balancing the interests of an American citizen on vacation in the Caribbean, or traveling to visit their uncle overseas in Canada, or whatever, against the abso-

lute necessity that we have the tools that we need to combat the threat of agencies and organizations abroad that wish to do us harm, that we have a reasonably good model in the balance that's been struck on the domestic side, through both the warrant requirement on the one hand and the minimization rules that protect the people who aren't the target, but happen to talk to the target on the other hand.

As a general proposition and allowing for the fact that there are going to be matters of fine legislative language and unintended consequences and so forth, as a general proposition does the Department of Justice agree that that is a useful and important benchmark in evaluating whether we have succeeded in striking that balance?

Mr. WAINSTEIN. I guess I'll draw on my personal experience, sir. I, like you and a number of members here, was a criminal prosecutor for 15 years of my career. I used Title 3. I used the regular warrant requirement in domestic law enforcement. It is what I was accustomed to. After 9/11, I got into the national security game and started seeing what was necessary. Frankly, I don't think that that construct would work. It simply would not work, given the volume, diversity of communications that we need to intercept, the nimbleness with which we need to act to protect.

Senator WHITEHOUSE. Wouldn't work for who? We have the Director of National Intelligence who said that Americans targeted abroad numbered 56. That is not in the context of our enormous defense effort against terrorism, in the context of our enormous—I think $40 billion-plus was recently declassified by the DNI intelligence effort against terrorism to pay for having people put together packages for 56 folks so that an American who travels abroad knows that they enjoy the warrant requirement, does not seem to be the kind of interference that you are suggesting. Why is it that putting together a package for 56 people would so offend that balance, in your view?

Mr. WAINSTEIN. No, I'm sorry. I was talking about a benchmark for signals intelligence, period, on the national security side.

Senator WHITEHOUSE. I'm talking only about American citizens.

Mr. WAINSTEIN. In terms of Americans—

Senator WHITEHOUSE. When they travel abroad.

Mr. WAINSTEIN. I recognize that that's a different kettle of fish and there are different rights implicated. My point is that—

Senator WHITEHOUSE. In fact, as far as we know, the U.S. Supreme Court might very well say that they have a warrant requirement right. It's never been decided otherwise, has it?

Mr. WAINSTEIN. No, you're right. It hasn't been decided. The problem is, there are operational concerns. One of the concerns, for instance, is in the amendment that passed there is no emergency provision for going up and surveilling a U.S. person overseas without going to the FISA court.

Senator WHITEHOUSE. I'm with you on emergencies. My time has run out. I thank the Chair.

Mr. WAINSTEIN. So I would be happy to brief you on other operational concerns we have about certain aspects of the amendment.

Senator WHITEHOUSE. We are in active discussion.

Mr. WAINSTEIN. Okay. Thank you, sir.

Senator WHITEHOUSE. Thank you, Madam Chair.

Senator FEINSTEIN. Thank you, Senator Whitehouse.

Senator Graham.

Senator GRAHAM. Thank you.

Thank you very much for your service to our country in many capacities. We have two concepts that have been competing against each other since 9/11, and I have somehow been able to make everybody on both sides mad at me at one point in time.

The first concept is that we are at war, which I agree. Some people in the administration had the view that when we are at war, there is only one branch of government. That is one of the reasons we have had this big fight, is because we've been fighting against a theory of the executive branch in a time of war that said there's no need for FISA or any other check and balance.

Did you ever feel comfortable personally with the idea that, when we authorized the use of force, congressional use of force regarding Iraq, that Congress intentionally gave you the authority to avoid compliance with FISA?

Mr. WAINSTEIN. I've read the argument that the AUMF, right in the aftermath of 9/11—

Senator GRAHAM. I mean, do you personally feel comfortable with that legal reasoning?

Mr. WAINSTEIN. I'd have to say, and I'm not just trying to hedge, I'd really have to go back and dig into it because it's a complicated matter. I don't pretend to be a constitutional scholar on the separation of powers issues, at least I don't have it at my fingertips.

Senator GRAHAM. I just want you to understand—I think you've been a very good witness—that one of the conflicts we've had, is that I'm a conservative, want to win the war as much as anybody else, but one thing that conservatives and liberals have in common is a concept of checks and balances, that we can have military—see, I think we're at war and the military should try these people that are caught who are suspected of war crimes, but there is a process that you go through with court review. So that's one concept that I think is now behind us, so I want to put on the record that I appreciate the administration's willingness to abandon that theory, sit down with us, and try to find a way to comply with FISA.

Now we've got another concept that I think is rearing its head in this debate, is that you're trying to apply domestic criminal law to a war-time environment. I have been arguing very ferociously that we are dealing with an act of war after 9/11, and the Law of Armed Conflict applies, not domestic criminal law.

I am the first one to say, you cannot hold someone indefinitely under domestic criminal law without a habeas petition or some court date. But we are not dealing with common criminals, we are dealing with warriors who can be kept off the battlefield, under the Law of Armed Conflict, for an indefinite period because it would be silly to release people back to the fight who have vowed to kill you.

Now, looking at FISA from those two concepts, the Protect America Act, I think, has found a sweet spot as far as I'm concerned. The general idea that you would need a warrant to surveille the activity of an enemy combatant justifies all the laws of armed conflict. So, as I understand this compromise we've reached, if you

find, or we find someone we suspect of being part of the enemy force, we have the ability to listen in to those communications under the theory that we are surveilling somebody who is part of the enemy. Is that correct? I mean, that's why we're following these people.

Mr. WAINSTEIN. It's for foreign intelligence purposes. Yes.

Senator GRAHAM. Yes. We're not following them for crime purposes, we're following them because we're at war.

Mr. WAINSTEIN. It's a matter of national security and foreign intelligence.

Senator GRAHAM. Right.

Mr. WAINSTEIN. I mean, that person can also be committing a crime at the same time. Of course, international terrorists are both a national security threat, as well as a criminal threat.

Senator GRAHAM. Right. Right.

Now, when an American is involved, here's where I think we need a warrant. If someone is calling me from overseas and you think the person calling me is a terrorist, I don't mind you listening in to what's being said. But if you believe I'm helping the enemy—and this gets back to your question—that I am somehow part of a fifth column movement, I want you to go get a warrant because you'd be wrong.

We've had examples of people since 9/11, anthrax, suspected of doing something. The government followed them around and nothing ever happened. I don't think it is a burden for the administration, this administration or any other administration, at a point in time to go to a court and say "we believe Lindsey Graham is involved with a terrorist activity".

Do you think that's a burden?

Mr. WAINSTEIN. No. That's a burden, actually, that we will shoulder, sir. Because, according to the legislation that came out of the Senate Intelligence Committee, if we want a target, when we get to a point where we're targeting somebody in the United States—

Senator GRAHAM. Right.

Mr. WAINSTEIN.—this is actually under the original FISA.

Senator GRAHAM. Right.

Mr. WAINSTEIN. But it continues through the Protect America Act. We have to go to the FISA court.

Senator GRAHAM. And that's really not a burden, is it?

Mr. WAINSTEIN. Well, it's a burden, but it's a burden that we assume and that we feel is appropriate, and that we're willing to carry on.

Senator GRAHAM. If you would have said that 3 years ago we wouldn't be doing all this.

Now, to my friends who want to expand it overseas, I think you are creating a burden. As much as I like Senator Wyden, we are at war. I do believe that his amendment is expanding FISA and doing the same type harm as if you never had to go through FISA. As much as I appreciate him, like him, and understand that he's doing this for all the right reasons, I hope we will find a way not to impose that burden upon our Nation at a time of war. That's just my comment, not a question.

Finally, about the retroactive liability of people who have helped us. What effect, if any—a chilling effect, if any—would it have that

if a company is held liable or can go to court by answering a request from their government with a document that says "this is a legal request", what type effect would it have in the future of the ability of this country to go get people to help us?

Mr. WAINSTEIN. From my personal, sort of parochial perspective, that is the big concern because, you know, I am in a division of people whose job is to enable the intelligence community to do fast, flexible surveillance when it's appropriate, and we're concerned that companies are rational beings. They say, Okay, we cooperated before, we then got taken into court, and all the damage that goes along with that.

Next time you come to us, it doesn't matter how good the form is that you give us, how strong an assurance there is, we're going to go ahead and litigate it all the way out to the nth degree to make sure that we protect ourselves and don't end up in court later on. That then delays our ability to go up and get the surveillance we need.

Senator GRAHAM. To my colleagues on the committee who think we're letting someone off the hook. I respectfully disagree. If we go down this road of holding people liable for answering a request of our government to help in a time of war, we're probably hurting ourselves, not letting someone off the hook.

Thank you.

Senator FEINSTEIN. Thank you very much, Senator Graham.

Senator Durbin.

Senator DURBIN. Thank you, Madam Chair.

Mr. Wainstein, when I use this little piece of technology to make a phone call or to send an e-mail message, I think I have a reasonable right to expect that that communication and my identity are going to be protected, confidential, private, except with some notable statutory exceptions. If the company that I'm doing business with receives a warrant to search or obtain records, that's understandable. At that point, their obligation to me as a customer is secondary to this warrant that they received.

Now, in this context of national security, under the statutes written, there is a second possibility. That is, in addition to a warrant, there could be this so-called certification that the government has the right to request this information, who I am, what I said, and what I did.

Now, you stated this in the most general terms in your testimony, in terms of the responsibility of the telecommunications provider to me, or any other customer. You said: "The committee's considered judgment reflects a principle in common law that private citizens who respond in good faith to a request for assistance by public officials should not be held liable for their actions."

So let me ask you this. In the course of our government's reaching out to telecommunications providers, asking for information about communications for the purpose of national security, did any of those telecommunications providers refuse to cooperate, refuse to provide the information?

Mr. WAINSTEIN. Senator, I'm just not going to be at liberty—or equipped, for that matter—to answer that question. Obviously it's classified. I wasn't even around during most of that, at least in main Justice. But I think that's something that you—I'm not sure

if you went to the briefing yesterday, but colleagues of mine were up there yesterday explaining the chronology and the history of the whole program, the terrorist surveillance program and the interaction with the providers, and we'd be happy to come up and answer any more questions.

Senator DURBIN. So in order to protect what was said at that hearing, let me continue on in a hypothetical way, noting that there has been one telecommunications provider through one of its officers who has reported publicly that they refused to cooperate. But let me ask you this. If the question is good faith on the part of the providers and we come to learn that a telecommunications provider refused to cooperate, saying that the certification that was provided by the government was not adequate under the law, is that something we should take into consideration?

Mr. WAINSTEIN. In deciding what sort of immunity and whether to—

Senator DURBIN. In deciding whether or not it's a good faith effort by a company to cooperate with government.

Mr. WAINSTEIN. Well, not knowing the facts and not being able to address the facts even if I knew them—I mean, the fact that a company refused doesn't necessarily make the rightness of their position. What I see, is that there are letters that went out to these companies that said very forcefully, this is being directed—this was directed by the President and this has been deemed lawful at the very highest levels of the government. That's a pretty strong assurance.

So I guess in terms of good faith, that's very strong evidence of good faith. The fact that one company refused to cooperate, if that is in fact the case, I don't think that necessarily undercuts the strength of those assurances.

Senator DURBIN. I disagree. If a telecommunications provider looked at the same certification as another telecommunications provider and concluded it was not sufficient under the statute to waive that company's responsibility to protect the privacy and communications of its customers, I think that is relevant to the discussion here.

Assuming for the sake of discussion this company that has already publicly disclosed what happened is factual in what they said, we at least know that one telecommunications provider took a look at what was being sent and said "that's not good enough. I have a responsibility to my customers to protect their identity."

So that raises a question of fact, doesn't it, as to what is good faith and what isn't. Which company operated in good faith? Where do we resolve questions of fact in America? Questions of fact and law are resolved in a court. What you're suggesting from your testimony is, we don't want to resolve this. We don't want to have these telecommunications providers held accountable to explain their conduct.

Now, that troubles me. It troubles me because, from my point of view, it's going to have a chilling effect on the relationship of telecommunications providers, their customers, and our government. How much can I trust in the future if I know the telecommunications providers can disclose my conversations, information about

me, with impunity, with immunity under the law? What do you think?

Mr. WAINSTEIN. Senator, thanks for that line of questions. Back to the fact that one company might have refused. Keeping it in the abstract, because I don't know the facts, it could be characterized that they did a good faith job and they determined that this wasn't sufficient. It also could be an example of the phenomenon I just described to Senator Graham, which is a company saying, boy, I'm just not going to do anything to assist the government.

I'm not going to make it easy. I'll go into my shell, and not try to help because I'm going to be risk averse. Well, the problem is, is that the more these companies are exposed, the more you're going to have companies doing exactly that. Now, I don't know what the thought process was in this particular case, but I'm saying that it could be—

Senator DURBIN. Interesting.

Mr. WAINSTEIN. It could be looked at that way.

Senator DURBIN. An interesting and relevant question. Isn't the law and fact usually resolved in a court, by a judge? And the point that was made earlier by Senator Leahy is that at some moment in time, after the public disclosure of the so-called "secret" program, our government decision, you know, the safest thing to do is to go through the FISA court. If we hand them a court order, we don't have to worry about whether or not this authorization document is really going to carry the day. That, to me, was a conclusion and an admission of the obvious.

That is an admission which I think shows where our government should have been from the start. They knew that if they went through the FISA court with a court order, the telecommunications provider would have no argument. But when you get to this so-called authorization, there clearly was an argument, at least for one telecommunications provider.

So, you know, it strikes me as strange, middling strange, here, that we're in a position saying that this company that is supposed to protect my identity and my communications, if it asserts my privacy, my right to privacy over a government request, that somehow they're obviously not doing their "patriotic duty". That's how you referred to it, their "patriotic duty".

It's even been suggested by one of my colleagues here that these lawyers bringing this lawsuit, we've got to question whether they might be connected with terrorist organizations. Remember that? Remember that statement that was made earlier? Hasn't this gone pretty far afield from the fundamental question, the conflict between privacy and security? Isn't it reasonable to say that company has a statutory and personal obligation to me to protect my identity, and only to give it up for a legitimate, statutorily recognized purpose, a court order or a certification that they can stand behind?

Mr. WAINSTEIN. Just to be clear, I've not heard—and I've followed this primarily in the newspapers—of bad faith on the part of any companies. We're not trying to suggest—I'm not suggesting that at all. I think, actually, companies acted in good faith, and I do believe they acted out of patriotic duty, or sense of patriotic duty.

I think, though, the legislation in the Senate Intelligence bill is a good middle ground where it gives targeted immunity for the events after 9/11 where companies did act on these assurances—but then lays out, prescribes a course for those kind of defenses in the future. There's a second part which does that, which I think is quite sound because it says, look, we're going to deal with this one-shot problem post 9/11, between 9/11 and when we went to the FISA court or got FISA court approval, but then from here on out, this is the mechanism that we're going to use, and we'll do that without having to resort to the State Secrets Doctrine. I think that's a very sound approach.

Senator DURBIN. Thank you very much.

Thank you, Madam Chairman.

Senator FEINSTEIN. Thank you, Senator. Thank you, Mr. Wainstein.

Senator Hatch has not yet had his first round. But before turning to him, I would like to state what the Chair's intent is. If anyone disagrees, please let me know. I'd like to go until 1:45, and we have a second panel. We'll ask the panelists to think about their remarks—we have their written remarks—summarize them, and then limit the rounds to a strict 5 minutes, if that's agreeable with everybody.

[No response].

Senator FEINSTEIN. Hearing no objection—I meant 12:45. Excuse me. Hearing no objection, that's the way we'll proceed.

Senator Hatch, it is all yours.

Senator HATCH. Well, thank you, Madam Chairman. I appreciate it.

I am sorry to keep you a little longer. But the current bill provides authorization for the Attorney General and the Director of National Intelligence to direct in writing an electronic communications service provider to provide the government with all information, facilities, and assistance necessary to accomplish authorized acquisition.

However, I don't see that the bill language has specific non-disclosure language for these likely classified directives. Can you research whether this is needed and provide an answer to the committee's consideration of the bill?

Mr. WAINSTEIN. [microphone off].

Senator HATCH. Okay, if you would.

Now, there have been some suggestions to have the FISC assess compliance with the targeting and minimization procedures. There are numerous oversight mechanisms in this bill already. Wouldn't this put the FISC in a position where it is making foreign intelligence determinations in place of analysis?

Mr. WAINSTEIN. That is the problem, that it would get the FISC in a position of being operational to the extent that it is not when it assesses compliance for, let's say the minimization procedures in the typical, traditional FISA context where you're talking about one order, one person. Here, some of our orders might well be programmatic, where you are talking about whole categories of surveillances. That would be a tall order for the FISA court to assess compliance.

Senator HATCH. That's my understanding. The House bill on FISA requires that the FISC approve any foreign targeting before it occurs. We need to remember, we're talking about foreign targets that are overseas. From the Department of Justice's perspective, what are the negative consequences of prior approval?

Mr. WAINSTEIN. It's that, prior approval raises a host of issues. One, we might not get the approval and that can slow things down. The House bill actually says, if at the end of 45 days the court hasn't ruled, our surveillance has to go down. There is an emergency procedure, but it goes down and we lose it. There's not even an mechanism for surveillance remaining up as we appeal a declination by the FISA court.

We have seen over time, as we've discussed earlier, as FISA has migrated—the jurisdiction of FISA has migrated to surveillances outside the United States with the change in technology since 1978, more and more we've had to go to the FISA court to get approval at the front end, and that's more and more burden on us and more—

Senator HATCH. And it always takes a considerable amount of time to go through the FISA procedure, sometimes less than others. But if it's a serious request, it can take a number of days, couldn't it?

Mr. WAINSTEIN. Yes. It can take a long time. It can also take a lot of person hours because you have to put together a lot of paper.

Senator HATCH. But we could lose the intelligence that really might protect our country.

Mr. WAINSTEIN. That's the concern. Yes, sir.

Senator HATCH. That's my concern. Other legislative proposals relating to FISA modernization have called for a narrow definition of foreign intelligence information applying only to international terrorism. Now, please provide an explanation of the flaws in this suggestion and how this type of unnecessary limitation could facilitate our intelligence community missing the next step?

Mr. WAINSTEIN. That's an interesting question, sir. For instance, the bill that the House is considering would take the definition of foreign intelligence information that is in FISA that talks about all of the sorts of information that you would think would relate to the national security, but would carve out, leave out of that definition in the House bill intelligence relating to the foreign affairs of the country.

Other bills have said, let's just limit this to international terrorism, not all the other types of foreign intelligence. The reality is, our foreign intelligence collection network and our intelligence community operates in a way that it gets the whole range of foreign intelligence—

Senator HATCH. Sometimes those ranges are interconnected that would lead to terrorism to begin with. You might not get the terrorists without the other range of information. Is that right?

Mr. WAINSTEIN. Absolutely. And to try to draw lines, to have analysts draw lines and say, well, this is more of interest to the State Department than the Defense Department, therefore it's foreign affairs and we can't do it, it would be very problematic operationally.

Senator HATCH. Yes. We're living in the big-time world here where we have a lot of people who'd like to destroy the United

States and everything we stand for, and our allies as well. We have to stand tough on these things. Is that a fair analysis?

Mr. WAINSTEIN. I agree sir. And you can bet that our adversaries, especially those other states who are directing intelligence operations against us, they are definitely trying to get all foreign affairs information and they're not limiting themselves.

Senator HATCH. They're not limiting themselves just to terrorism.

Mr. WAINSTEIN. Not at all.

Senator HATCH. Because they don't have a threat from us.

Mr. WAINSTEIN. Right.

Senator HATCH. Well, this legislation is crystal clear about prohibiting reverse targeting. Testimony in the second panel leads me to believe that people still don't understand that particular issue. Now, can you describe for us reverse targeting and how it is not allowed under current law, as well as this legislation?

Mr. WAINSTEIN. Thank you for that question because it is, understandably, a complicated area. What it means when we target somebody for surveillance, it means—and this is very operational—the intelligence community actually takes its gizmos and targets them against the person or the facilities that person is using outside the United States, so under this legislation we would be able to do that without going to the FISA court.

Senator HATCH. Right.

Mr. WAINSTEIN. The concern is, what we would do, is we'll find Ken Wainstein, who's outside the United States, and we'll target him, but we're doing that really because we want to get the communications of a person within the United States. So the concern is, we're actually using this to circumvent the court to actually surveille someone in the United States.

This legislation from the Senate Intelligence Committee makes it clear we cannot do that. Original FISA said we cannot do that. Once we target the person in the U.S., we have to go to the FISA court. And as a technical matter, targeting the person in the United States means a technical shift, so we're actually shifting our targeting and our apparatus over to that person. It's against the law to do that. We'd have to go to the FISA court.

In fact, it would make no sense, sort of as a matter of tradecraft, if we really had an interest in the person in the U.S., to just limit our surveillance to the person who's outside the U.S. and talking to him, because we'd only get that suspect's communications to the person outside the U.S. You wouldn't get all that other person's communications. Instead, what we would do is go to the court and get a FISA order to get all that person's communications. So this legislation makes clear we can't do that, FISA made it clear we can't do that, by letter from us to this committee a couple of months ago we made it clear we're not doing it, we won't do it, and congressional oversight will ensure that we won't.

Senator HATCH. Madam Chairman, could I have just a little of additional time to make a comment or two that I'd like to make?

Senator FEINSTEIN. Yes.

Senator HATCH. I appreciate your testimony and I appreciate the difficulties in these areas. I hope that people aren't going to try and exploit some of these situations because we are talking about pro-

tecting people in this country and our allies around the world. It takes an awful lot of effort. Unfortunately, more has been disclosed about what we have been trying to do than I think should have been disclosed.

Section 703(c) of this bill has received a great deal of attention, with good reason. This section would require court approval for acquisitions targeting American persons overseas. Unlike current provisions of FISA relating to electronic surveillance, this section provides no emergency provision for an acquisition targeting an American citizen overseas. Now, this means that it would be harder to surveille a citizen outside of the country than inside the country. Do you agree with that?

Mr. WAINSTEIN. Yes. That's the irony of it.

Senator HATCH. Given the importance of intelligence collection to our safety, why in the world would we handcuff ourselves in this way? I mean, even if this section is amended, it is a dramatic departure from the 26 years of history under Executive Order 12333. I think it's imperative for us to emphasize that there are many warrant exceptions to the Fourth Amendment.

The question is whether the search is "reasonable". For example, the individuals attending today's hearing were forced to go through a magnetometer just go get access to this building. Now, this was a warrantless search, but I think everybody would agree that it's a reasonable search.

So if the Attorney General of the United States determines via probable cause that an American citizen overseas is an agent of a foreign power, is a warrantless acquisition of his communications reasonable? I think the answer is an emphatic "yes". Do you agree?

Mr. WAINSTEIN. Yes, sir. And I think that's the basis for the 12333 mechanism that has been in place. As you point out, there are many scenarios where a search is done: at border searches, stop points where they stop cars, whatever the term is, here going in and out of public buildings where there are searches. They are done without court order, but they're considered "reasonable". Reasonableness is the touchstone. That's the critical element for searches overseas, and that is satisfied by this 12333 mechanism. It's been found that way by the court.

Senator HATCH. I'm grateful to the Chairman for giving me a little extra time.

Could I put this in the record?

Senator FEINSTEIN. You certainly may, Senator.

Senator HATCH. Madam Chairman, I would like to put in the record the October 29, 2007 letter from James B. Comey, former Deputy at Justice, John Ashcroft, the former Attorney General, Jack Goldsmith, who has been quoted in the media continuously, and Patrick F. Philbin.

[The letter appears as a submission for the record.]

Senator HATCH. This letter is directed to the Chairman and Ranking Member, Chairman Leahy and Ranking Member Specter. It's written to support the carrier immunity provision, passed with bipartisan support in the FISA reform legislation recently reported out of the Senate Select Committee on Intelligence and now before your committee for consideration.

It is a very interesting letter and makes a very good case that we're talking about protection of our people in this country. If we don't get the tools to protect, and if we don't have access to the telecom companies and others, if they are going to be sued, there's $40 billion worth of suits because they cooperated with our intelligence community, if we don't give them immunity there isn't going to be any cooperation in the future. How would that affect us?

Senator FEINSTEIN. Senator, your time—I've been very generous.

Senator HATCH. You have been. I think—

Senator FEINSTEIN. I'm just—

Senator HATCH. I think I'll have to quit at that question.

Senator FEINSTEIN. I think you might be well advised.

Senator HATCH. Okay. Well, if you answer that, I'll keep my mouth shut and I won't even ask for a second round.

Senator FEINSTEIN. Quickly, Mr. Wainstein.

Mr. WAINSTEIN. It will detrimentally affect us, Senator Hatch. Very much so.

Senator FEINSTEIN. You've got the answer, Senator. Thank you very much.

Senator HATCH. Thank you.

Senator FEINSTEIN. Senator Brownback.

Senator BROWNBACK. Thank you very much, Madam Chairman.

Mr. Wainstein, thank you for your testimony. I've just got a couple of points and they're ones you've covered, but I just want to make sure that I'm clear on it and I understand you fairly as well.

One, just really following up with Senator Hatch's thoughts, we're going to be in this fight on terrorism, I think, at least for a generation. If we don't have private companies, private individuals cooperating with us, I think we're going to have a longer fight, and we'll have a less successful fight.

And so we've got to give them some liability protection to be willing to work with us. That's why I like to see the provision in the bill. The FISA Amendment Act goes, I think, a long way toward giving the intelligence community, which plays this vital role of protecting the lives of Americans and our neighborhoods around the world, the tools it needs.

I am especially pleased that the Act provides liability protection for the communications service providers. I just think that is incredibly important. A guy yesterday was telling me that telecommunication intelligence is the queen on the chessboard now for us. With the difficulty of human intelligence, this is just key. We've got to be able to get at this information and we've got to be able to protect people's civil liberties.

I agree with all of that. I just want to make sure, from your perspective, just to be clear, this bill does not grant any immunity for criminal acts that might be done by private individuals.

Mr. WAINSTEIN. No, sir, it doesn't.

Senator BROWNBACK. Okay. And it does not grant immunity for any government agencies or officials?

Mr. WAINSTEIN. No. It's for the providers.

Senator BROWNBACK. Okay. So even with the carrier immunity, there are still avenues for individuals to challenge actions that might take place. Is that correct?

Mr. WAINSTEIN. Absolutely. I think, actually, if people have concerns, it's about the legality of the program as determined by the government. So if they're going to litigate, they should direct their litigation at the government that assured the providers that this was legal.

Senator BROWNBACK. It sure looks like to me, if we don't provide this liability immunity to the communications companies, they're going to start turning us down for a request for information that we should be able to lawfully obtain. Is that correct?

Mr. WAINSTEIN. That's my concern, that they'll turn us down or they'll just feel like, to protect themselves against potential liability down the road, they've got to litigate everything we give them. They've got to challenge every order, every directive just to make sure that if someone down the road sues them, they've got a record, a record of having pushed every button and made sure that they've looked at every angle. That is—

Senator BROWNBACK. That eats up time.

Mr. WAINSTEIN. It eats up time.

Senator BROWNBACK. That takes us away from being able to get the intelligence information that is probably in a real-time need, would be my guess.

Mr. WAINSTEIN. Absolutely. When we hear about a facility we want to surveille, we need to go up immediately. That's why we use the emergency authority quite often. But just like criminals who go through telephones all the time, change their phones all the time, terrorists will change their modes of communication. So if we can't get up and going on them quickly, we often lose the opportunity to get the information we need.

Senator BROWNBACK. And for us to be able to get the private sector cooperation, they need the liability limitations or the liability immunity. Is that correct?

Mr. WAINSTEIN. Yes, sir.

Senator BROWNBACK. As a lawyer who does not practice this type of law, but if I were advising a company without that liability limitation or immunity exposure, I would just say "don't do it". The safe answer is "no". The safe answer is to make them go through the court system. I just don't know why anybody would cooperate with us without that.

There was a great piece in the Wall Street Journal today. It was former Attorney General Civiletti and Thornburgh, former FBI and CIA Director Webster that wrote this: "The government alone cannot protect us from the threats we face today. We must have the help of all our citizens. There will be times when the lives of thousands of Americans will depend on whether corporations, such as airlines or banks, are willing to lend assistance.

If we do not treat companies fairly when they respond to assurances from the highest levels of the government that their help is legal and essential for saving lives, then we will be radically reducing our society's capacity to defend itself." I don't know if it could have been put any more clearly or succinctly. I presume you would agree with that statement.

Mr. WAINSTEIN. Absolutely. It's stated much better than I've stated it here today. But that is the point, that we run the risk of really handicapping ourselves in the war on terror.

Senator BROWNBACK. Madam Chairman, thank you for this chance. Mr. Wainstein, thank you for your work. Godspeed.

Mr. WAINSTEIN. Thank you very much, Senator Brownback.

Senator FEINSTEIN. The hour is upon us for you to depart. I want to thank you very much. I know the committee appreciates your testimony. So, thank you, Mr. Wainstein.

Mr. WAINSTEIN. Thank you very much, Madam Chairman. Thank you for the opportunity.

Senator FEINSTEIN. Thank you.

We will move quickly on the next panel. As they come up, I will introduce them.

Ed Black is the president and CEO of the Computer & Communications Industry Association, where he previously served as vice president and general counsel. Mr. Black also serves on the State Department's Advisory Committee on International Communications and Information Policy. Mr. Black spent time in the State and Commerce Departments during the 1970's, focusing on a range of issues, including telecommunications and technology policy. He has worked for two Members of Congress.

The next person is Patrick Philbin, who currently works at the law firm of Kirkland & Ellis. From 2001 to 2005, Mr. Philbin served in the Department of Justice, where he focused on national security, intelligence, and terrorism issues.

As a Deputy Attorney General in the Office of Legal Counsel from 2001 to 2003, a critical time, Mr. Philbin advised the Attorney General and counsel to the President on national security issues. As an Associate Deputy Attorney General from 2003 to 2005, he oversaw and managed national security functions of the Department, including applications for electronic surveillance under the Foreign Intelligence Surveillance Act.

Morton Halperin is the director of the U.S. Advocacy at the Open Society Institute, and the executive director of the Open Society Policy Center. Dr. Halperin has served in three administrations, with positions in the State Department, the National Safety Council, and the Defense Department.

Dr. Halperin has also worked for the American Civil Liberties Union, serving as director of the Center for National Security Studies from 1975 to 1992. He has taught at several universities, including Harvard, Columbia, and MIT. He has missed the West Coast in that area.

But we will now proceed. I will ask the panelists, beginning with Mr. Black, to try to confine their remarks to 5 minutes, and then we will followup in like manner.

Mr. Black?

STATEMENT OF EDWARD BLACK, PRESIDENT AND CEO, COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION, WASHINGTON, D.C.

Mr. BLACK. Thank you, Senator Feinstein. It's a pleasure to be here. I am Ed Black, president and CEO of the Computer & Communications Industry Association.

For 35 years, CCIA has consistently promoted innovation and competition through open markets, open systems, and open networks. We greatly appreciate the opportunity to discuss the critical

intersection of national security law and privacy rights before this committee.

As we all know, the Internet is an unprecedented and unique force for democratic change and socioeconomic progress. Increasingly, our Nation's digital economy—indeed, our global competitiveness—depends on the dynamism and openness of the Internet.

In the digital economy, all information service companies have a custodial role to play regarding two key fundamentals of the Internet: free speech, as protected by the First Amendment, and privacy and security, protected by the Fourth.

If the marketplace loses confidence in the security of business and personal transactions online, the entire digital economy could grind to a halt. We understand our industry's technology and the many ways in which it can be used, and ways it can be misused. In addition to the most obvious domestic benefits, the Internet is a tool for spreading freedom and democracy around the world. Indeed, our government must continue to lead by example in promoting the freedom of ideas and communications that the Internet makes possible.

We urge you to ensure that this legislation not weaken the hand of American companies that must contend with escalating demands for censorship and surveillance by foreign secret police around the world. CCIA supports current legislative efforts to amend FISA to achieve a sound balance between effective terrorist surveillance, vital to our national security, and the constitutionally protected rights to privacy and free speech.

We want to be good citizens. We do not, however, want to be police agents. In order to do that, we need protection not just from third party liability for acquiescing to proper demands, but protection from improper government pressure or inducements as well.

The Senate Intelligence Committee legislation, S. 2248, while providing some important improvements over the hastily passed Protect America Act, will allow too much surveillance of Americans based on executive certification without a court order, and disturbingly, the bill provides retroactive immunity from civil liability for those who may have participated in any illegal program without a full understanding of what conduct is being immunized.

If we continue to make up the rules as we go along, any violation of the Constitution perform to serve a very tempting national security or law enforcement purpose and can be rationalized and covered up by retroactive immunity. Retroactive immunity for participation in the recent secret government surveillance program is premature at best.

If immunity for past activities is granted prior to full disclosure and accountability, Congress and the public may never understand the real nature of the NSA warrantless wire tapping program. We also believe broad retroactive immunity would be ill-advised in any event because it would perpetuate uncertainty, confusion, and second-guessing in the future. If retroactive immunity is granted in this case, future extra-legal requests will be accompanied by a wink and a promise of similar immunity after things settle down.

Civil litigation should be allowed to proceed. Even if major portions of the proceedings need to be held *in camera* and the scope of discovery narrowed, judges—and to the extent compatible with

serious national security concern, the public—should, and needs to, learn what really happened in these cases.

In conclusion, millions of workers in our industry believe that we are an industry that can be a strong, positive force for our society. The underlying desire to facilitate communications, the transfer of information and knowledge, and the building of bridges across cultural boundaries: these are core motivations of people in our industry. These motivations are part of why our industry is successful. The economic rewards can be great, but they are as much a consequence as they are a motive.

To sustain this positive force, we must work together to establish processes and protections for private, personal, and business information that is so critical to the open and free use of the Internet. Our industry needs clear and constitutionally proper ground rules that are only deviated from through well-defined, transparent processes. These rules must be straightforward enough to be publicized and understood by U.S. citizens and business people who may be called upon to assist their government in these uncertain times.

Thank you.

Senator FEINSTEIN. Thank you, Mr. Black. And thank you for coming so close to the time limit. I appreciate it very much. Excellent testimony, too.

[The prepared statement of Mr. Black appears as a submission for the record.]

Senator FEINSTEIN. Mr. Philbin.

STATEMENT OF PATRICK F. PHILBIN, PARTNER, KIRKLAND & ELLIS, WASHINGTON, D.C.

Mr. PHILBIN. Thank you, Madam Chairman. I will try to keep on the time limit as well.

I gained experience related to FISA and electronic surveillance during my service at the Department of Justice and learned that electronic surveillance is a vital intelligence tool.

At the same time, it's an intrusive technique that if not constrained and controlled properly, can threaten the liberties and privacy of American citizens. Ensuring that electronic surveillance remains an agile and adaptable tool, while at the same time protecting American liberties, is the challenge Congress faces in amending FISA.

In my testimony, I'd like to cover three points related to bill 2248. First, I want to express support for the provisions in the bill that will allow the executive to target the communications of persons reasonably believed to be overseas without first going to the FISA court. These provisions are consistent with FISA's original purpose and are necessary to ensure that FISA does not fall out of step with changing technology.

FISA was not meant to regulate the collection of intelligence on the communications of persons overseas. Changing technology has led to the fact that some communications going through the United States are now under the FISA court jurisdiction. In my view, given changes in technology, a longer term solution to make the application of FISA less dependent on the medium used to carry a communication, such as wire versus radio, and more directly tied to the location of the target, is definitely warranted.

This provision is a good start in that direction. It appropriately addresses the Nation's intelligence needs, especially during the ongoing conflict with Al Qaeda, where speed and flexibility in responding to targeting and tracking of subjects overseas are vital for intelligence success.

Second, I want to express my support for the provisions in the bill that grant immunity to telecommunications carriers against lawsuits based on the carriers' alleged participation in intelligence activities involving electronic surveillance authorized by the President. I think that that immunity is warranted for several reasons. First, protecting the carriers who allegedly responded to the government's call for assistance in the wake of the devastating attacks of 9/11 is simply the right thing to do.

The allegations here are that, in the wake of 9/11, corporations were asked to assist the intelligence community based on a program authorized by the President himself and based on assurances that the program had been determined to be lawful at the highest levels of the executive branch.

Under those circumstances, corporations should be entitled to rely on those representations and accept the determinations of the government as to the legality of their actions. It would be fundamentally unfair, in my view, to simply leave those who relied on representations from the government twisting in the wind.

The fundamental notion of fairness here is also rooted in the law. As was mentioned in an earlier session, there is a common law immunity for those who assist a public officer who calls for assistance in a time of crisis. It is the same principle of fairness that applies here.

Second, immunity is appropriate because allowing the suits to proceed would risk leaking sensitive national security information. As the suits progress, they will inevitably risk disclosure of intelligence sources and methods that will damage the national security. The assertion of state secrets privilege is not a cure-all here. If it were a cure-all, the litigation would not still be proceeding 2 years after it was filed.

The longer the suits proceed, the more details concerning the ways the intelligence community may seek information from the Nation's telecommunications infrastructure will leak. Our enemies are far from stupid. As such information trickles out, they will adapt their communications security to thwart our surveillance measures and valuable intelligence will be lost.

Third, failing to provide immunity to the carriers here would discourage both companies in the communications sector and other corporations from providing assistance in the context of future emergencies. In the continuing conflict with Al Qaeda, one of our Nation's greatest strategic assets is our private sector and the information it has available to it.

Intelligence is vital for success in this conflict, and particularly communications intelligence. If immunity is not provided, however, it is likely that in the future private sector corporations will prove much more reluctant to provide assistance swiftly and willingly, and critical time in obtaining information will be lost.

I agree fully with the conclusion in the report in the bill from the Senate Select Committee on Intelligence that "the possible reduc-

tion in intelligence that might result from this delay is simply unacceptable for the safety of our Nation."

Finally, I disagree with the suggestion made by some that carriers should be forced, through the threat of liability, to serve a gatekeeper role to second guess and provide, in essence, oversight on the intelligence-gathering decisions of the executive. Communications companies are simply not well-positioned to second-guess government decisions regarding the propriety or legality of intelligence activities.

I know from experience that the legal questions involved in such matters are highly specialized, extremely difficult, often involve constitutional questions of separation of powers that have never been squarely addressed by the courts, and are not readily susceptible for analysis by lawyers at a company whose primary concern is providing communications service to the public.

Conducting the complete legal analysis, moreover, requires access to facts and intelligence information that is not, and should not be, fully shared outside the government. We should not adopt policies that effectively require private corporations to demand intelligence information from the executive and to conduct their own mini-investigations into the propriety of intelligence operations. At the same time, there must be some mechanism for addressing concerns raised about the intelligence activities at issue.

As the committee is likely aware, I am intimately familiar with the legal analysis conducted within the executive branch, and debates about that analysis. I can understand that reasonable people want further probing into the legal basis of the program, and ensuring that all intelligence activities do strictly adhere to the law is an imperative.

But the question of liability for telecommunications carriers is logically and legally distinct from that debate. The mechanism for addressing legal concerns about the intelligence programs is through rigorous oversight within the executive branch and through a joint effort between the executive and Congress to ensure appropriate oversight. The executive and Congress is charged with that responsibility. Private lawsuits are not the best mechanism for providing that oversight.

In conclusion, Madam Chair, I'd just like to note that I agree with the comments that were made earlier, that a warrant should not be required from the FISA court for conducting surveillance of a U.S. citizen overseas. That is an expansion of the FISA court's authority that I believe is unwise.

Thank you.

Senator FEINSTEIN. Thank you, Mr. Philbin.

[The prepared statement of Mr. Philbin appears as a submision.]

Senator FEINSTEIN. Dr. Halperin.

STATEMENT OF MORTON H. HALPERIN, DIRECTOR OF U.S. ADVOCACY, OPEN SOCIETY INSTITUTE, WASHINGTON, D.C.

Dr. HALPERIN. Thank you very much. I want to note that there are, of course, many other people and many other organizations that are expert on this and have deep concerns about it. I know it was not possible to have them all as witnesses, but I trust the committee will look at those views as well.

I want to focus on the issue of immunity and the question of sole means, because I think they're very closely related. The discussion we've had this morning is a logical one, but it totally ignores the history and the legislation that is before us. It ignores the history because we were at exactly the same point when FISA was introduced.

I was very much a part of that debate. The phone companies came in in exactly the same way. They were being sued. I had sued them for participating in the wire tap of my home phone. They said this is unreasonable. We should not be required to second guess. When we get a request from the government, we should be able to know very clearly what we're supposed to do.

Congress provided that answer with extraordinary clarity in the FISA legislation. It said, if you have a FISA warrant or a certification from the government that the specific provisions of FISA which permit surveillance without a warrant have been met, if you get one of those two things, you must cooperate.

If you get something else, like a certification that says the President has decided this is lawful without citing a statutory provision, then they were supposed to say no, and they were subject to civil and criminal penalties if they did not, both State and Federal civil and criminal penalties.

I think the law was absolutely clear. So to now cite the common-law rule that you need to cooperate, or say it is unreasonable to put phone companies in this position, ignores the fact that Congress answered that question with great precision in FISA. It is also illogical, the argument that's being made, because the argument says we want them to cooperate in the future, and therefore we have to give them this immunity.

But as the witness from the Justice Department agreed—and I thought that was very important—this bill does lay out for the future a scheme which does not require the phone companies to do any of their own analysis or to make their own judgment about what is patriotic.

Now, paradoxically it's the same scheme that was in the original FISA, but a little clearer. I think there are ways in which you can go beyond the Senate Intelligence Committee bill to make it even clearer that Congress means to say to the phone companies, you either have a warrant or you have a certification that a specific provision of FISA where you don't need a warrant is involved. If you get one of those two you must cooperate, and if you do not, you may not cooperate.

Now, that's a rule going forward which will lead the phone companies to cooperate because there's no judgment. So the logic that says we need to give them immunity about the past so that they'll cooperate in the future makes no sense, because we're telling them to cooperate in the future not if they get another plea that the common law requires them to cooperate, but only if the government meets the standards for the certification. So, I would urge you to build on what the Senate Intelligence Committee did and add to those provisions.

Another very important provision, in my view, is the question of how you avoid them using this when the real interest is a U.S. person. Again, I think we had very important testimony from the Jus-

tice Department saying that when a U.S. person becomes of interest to the intelligence community, we need to get a warrant from the FISA court, and we want a warrant because we want all of his conversations.

That is the language that is in the House bill. The House bill says that when a person in the United States becomes—a significant reason to do the surveillance is because you want information about a person in the United States, you need to get a warrant from the FISA court. I would urge you to add that to the bill. It changes nothing. It's exactly the assurance you were given from the Justice Department. But it makes it a statutory requirement and puts the FISA court in the process of making sure that when the purpose is to learn about an American, a person in the United States, then you need a warrant.

Finally, more generally, I think you do need to give the FISA court some additional leeway so that it can supervise the process. As we heard in one of the exchanges, the way the bill is written, even if the FISA judge decides that the minimization procedures are being violated, there's nothing he can do. Now, I think a judge would say it doesn't matter; if this is before me, I'm going to decide it. But I think Congress ought to make it absolutely clear that the FISA court has to supervise all of the requirements of the statute.

Thank you.

[The prepared statement of Dr. Halperin appears as a submission for the record.]

Senator FEINSTEIN. Thank you all very much. Dr. Halperin, you speak very quickly, and I think very slowly, so we've got a little point here. In looking at your point on the warrant accompanying the certification with respect to the existing FISA law, and I'm looking at the law, it would seem to me, if one just added a few words to say that the warrant essentially must accompany—it's Section 2511(2)(a)II: "Notwithstanding any of the providers of wire or electronic communications services or officers, agents, landlords, custodians, other persons are authorized to provide information, facilities, or technical to persons authorized by law to intercept wire, oral, or electronic communications, or to conduct electronic communications as defined. . .only if such provider, its officers. . . have been provided with a court order directing such assistance." So we would only have to add one word, "only".

Dr. HALPERIN. Well, I think "only" is important, but you certainly could add it. The other change I think you make, and need to make, and it's one of the four I lay out in my testimony, is indeed which talks about a certification as the alternative to the warrant. It says that "no warrant or court order is required by law." I think you need to say "by this law" and that "all statutory requirements of this statute have been met, and that the specific assistance is required", so that you make it clear that a certification has to be based on a specific provision.

For example, you say in an emergency you can go by a certification, or for the least—in the original FISA you can go by a certification. So I think with those changes in these words, you would eliminate some ambiguity, and I suggest specific language in my testimony.

Senator FEINSTEIN. Thank you.

Mr. Philbin, what do you think of that?

Mr. PHILBIN. Madam Chair, I am not sure, responding on the fly, that I have a very well thought out response. But it is certainly true that the interaction between 18 U.S.C. 2511 and FISA is complex and that is the key for determining how effective any exclusivity provision is going to be, which I understand to be your concern. I think it would be a mistake to change the provision in 2511(a)(2) to restrict the way that the certification immunity there is provided. I think that that's been in the law for a long time. It's been in the law for a long time for a reason.

Senator FEINSTEIN. Except now the terrorist surveillance program, all of it, is under FISA, you know. One doesn't know what the court would have done way back when, but it certainly was worth a try, which didn't happen. It seems to me that what Dr. Halperin has suggested, and in a sense Mr. Black suggested it as well, is really the way to handle this, that the Presidential certification doesn't necessarily provide the guarantees to the telecom—it certainly doesn't this time, and I've read it—so therefore it seems to me the court does provide the guarantee to the telecoms and the court does provide the guarantee to the individual citizen. So why not do that? Because one of the things we're going to try to do, I believe, is put as much of this type of intelligence collection under FISA as possible.

Dr. HALPERIN. Could I just add one point?

Senator FEINSTEIN. Sure.

Dr. HALPERIN. I think I very much agree with that. That's why I urge you to require that the government get a FISA order before it begins the surveillance authorized by this program. The government has now conceded a major role for the FISA court, and provided you have an emergency provision, I see no reason why you should not say, go to the court first and get this warrant, precisely because it then says to the court—it says to the providers, if there's a warrant you do it, if there's no warrant you don't do it.

Senator FEINSTEIN. And the court will give what I call a program warrant.

Dr. HALPERIN. Right. Exactly.

Senator FEINSTEIN. So that's what you're looking for. You're looking for the court oversight, and then the court can set the strictures, say I want you to report to me every 3 months, every 30 days, whatever it is. But the court then can provide oversight protection. I don't think it hobbles the executive at all.

Dr. HALPERIN. I agree.

Senator FEINSTEIN. Does anybody differ with that? My time has almost run out.

Mr. PHILBIN. I think it is certainly an improvement in FISA to ensure that the court can provide programmatic approvals. I don't think—my personal view is that it is impossible to predict now every exigency of the future that may arise. I think that the legislative scheme—what you're talking about here is limiting the immunity, to cut down on the immunity in this 2511 provision going forward so that it specifies only certain certification, the specific certification in FISA or something to that effect, or a court order.

I can see that if the objective is to provide the immunity only where that kind of piece of paper is given, that it will achieve that

effect. But I don't think that it is possible to predict now every exigency that will arise in the future and say that FISA is going to have all of that covered.

Senator FEINSTEIN. Well, I guess that's where I really disagree with you. I mean, I think we've reached a stage, after the Shamrock investigation, the FISA bill, the prohibitions in FISA, the fact that here it happened, the executive made the decision not to go to the court—they didn't go to the court for a substantial period of time. They stopped the program, obviously feeling that it was legally vulnerable, and then they went to the court. I think that's a big lesson for us in drafting legislation to prevent this from ever happening again. My time is up.

Senator Specter?

Senator SPECTER. Thank you, Madam Chairwoman.

Mr. Black, I note that you worked with Secretary Kissinger during the Nixon administration. I think it may have been about the same time that Mr. Halperin was under surveillance.

Dr. HALPERIN. I was also working with Mr. Kissinger in the Nixon administration.

Mr. BLACK. And I should clarify, I only joined when President Ford took over.

Senator SPECTER. You were working with Mr. Kissinger, too?

Dr. HALPERIN. When he was the Director of the National Security Council in the first 9 months of the Nixon administration.

Senator SPECTER. Was Mr. Black under surveillance when you worked for Secretary Kissinger?

Dr. HALPERIN. I couldn't reveal that.

Mr. BLACK. I should clarify, I only joined that administration under President Ford.

Senator SPECTER. Mr. Black, was Mr. Halperin under surveillance when you worked with Secretary Kissinger?

Mr. BLACK. I'm glad to say I worked on nuclear proliferation and other related issues, so I have no idea. But I really only joined the administration following President Nixon's resignation.

Senator SPECTER. Did you enter a general "not guilty" plea?

Mr. BLACK. Definitely "not guilty".

Senator SPECTER. Mr. Philbin, why not indemnification? First, let me congratulate you for standing up as Mr. Comey lauded your performance under difficult circumstances.

Mr. PHILBIN. Thank you, sir.

Senator SPECTER. That is most commendable and rare. So, thank you. But why not? Why not indemnification? Will there be realistic losses to the government by these lawsuits which will be defended with every procedural device known?

Mr. PHILBIN. I don't think that the problem with indemnification as a solution is ultimately the payout of money. That's not the concern. The problem with indemnification is that the lawsuit still has to proceed with the carrier as defendant, so the carrier is bearing all the burdens of litigation, which are significant.

Senator SPECTER. But there is a Motion to Dismiss on grounds of state secrecy. The carrier never appears.

Mr. PHILBIN. And if state secrets had really been a cure-all, a silver bullet for these cases, they would be gone by now, I think. I mean, they've been pending for 2 years.

Senator SPECTER. Well, what's happening with it? Anybody collected anything?

Mr. PHILBIN. That's part of my point, Senator. It's not the money that is really the problem here. It's part of the problem, but it's the burden of the litigation itself. The cost of going through the litigation itself, reputational and other harm to the companies of going through the litigation, and damage to the United States in the form of potential leaks of national security information during the litigation. And—

Senator SPECTER. What information is going to be disclosed? We couldn't even get it disclosed to the Chairman of the Judiciary Committee.

Mr. PHILBIN. That, Senator, though, was based on a decision of the executive, that the executive was in control of. This will be a decision by an Article 3 judge, and there's one Article 3 judge that, in one of the cases, already rejected the assertion of the state secrets privilege because a certain amount of what has become known as the terrorist surveillance program was already publicly described. And—

Senator SPECTER. Well, the Article 3 judges aren't always right, but I think they've traditionally provided good balance.

I only have a minute and 40 seconds left, and I want to ask Mr. Halperin a question or two. Mr. Halperin, what about Article 2 power? The Foreign Intelligence Surveillance Act provides the exclusive remedy, but doesn't the President have Article 2 power, as Circuit Courts have said, weighing the national security interest versus the invasion of privacy that supersedes the statute?

Dr. HALPERIN. Well, first of all, almost all of the Circuit Court decisions are pre-FISA decisions and held that in the absence—

Senator SPECTER. Almost all, but not all.

Dr. HALPERIN. Not all of them. But there are one or two in the other direction as well. So I think the Supreme Court has never spoken on this, nor come close to speaking on this question. But I think—

Senator SPECTER. I'm not talking about the Supreme Court speaking, I'm asking you to speak. Isn't there Article 2 power?

Dr. HALPERIN. I think that there may be some extreme power, in some extraordinary situation when the country is directly under attack, for the President to act. I don't think you can take—as you say, and as the Senate Intelligence Committee says, whatever power there is, you can't take away, nor can any President promise that future Presidents won't claim it.

But what I think the Congress clearly has the right to do, is to educate the rules for the service providers. I think you can lawfully tell a service provider that, you cooperate with a warrant or a certification provided by this statute or the Federal Government or the State government can put you in prison.

Senator SPECTER. Mr. Halperin, I have only 13 seconds left.

Dr. HALPERIN. I'm sorry.

Senator SPECTER. So I'm going to ask a question before my red light goes on. You want to limit it to counterterrorism only instead of all foreign information gathering. Why shouldn't we try to listen to what Iran is doing about a nuclear weapon?

Dr. HALPERIN. We should try to listen to that, and we've listened to that under FISA. We listened during the cold war to the Soviet Union and we had successive directors of Central Intelligence saying those rules worked. There are different problems when you're dealing with terrorists who are trying to conduct operations within the United States. I think Congress should be open to amendments that respond to the specific problem of terrorists in the United States. But the old rules were good enough for the Soviet Union. I think they should be good enough for information about Iran or other foreign powers.

Senator SPECTER. Well, I have many more important questions to ask, but I believe in observing the red light.

Senator FEINSTEIN. Wow.

Senator SPECTER. And I will say only one thing in conclusion. I regret the ways of the Senate that keep you sitting here for several hours, and then only have two of us appear to question you. I regret that. But it is a very busy Senate and this happens, regrettably, all the time. So although you have not been treated as you should be, you have not been discriminated against. It happens to everybody on the second panel.

[Laughter.]

Thank you.

Senator FEINSTEIN. I'd like to say thank you. I think your testimony was very important and gave us some good ideas. So, thank you very much.

The hearing is adjourned.

[Whereupon, at 12:58 p.m. the Committee was adjourned.]

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

QUESTIONS AND ANSWERS

Ed Black's Response to Sen. Brownback's Written Questions regarding the October 31, 2007 Senate Committee on the Judiciary Hearing regarding "FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability."

1. ***Is there any reliable evidence that any of the plaintiffs purporting to sue the carriers was actually surveilled by the NSA?***

   A: While media reports indicate that in at least one case the NSA surveilled plaintiffs, the administration's aggressive assertion of the common law State Secrets Privilege has limited discovery in many of the cases, thus preventing individuals from ascertaining for certain whether or not they were surveilled by the NSA. At least one former AT&T employee has come forward with evidence indicating that the NSA installed large surveillance networks in several US facilities, which had the capability of monitoring all private communications traffic that passed through those facilities.

2. ***Are there any other instances you are aware of where the law requires or expects private actors to second-guess governmental determinations that official actions are legal?***

   A: The Federal Rules of Civil Procedure and the Federal Rules of Criminal Procedures each permit parties to ascertain whether governmental requests for confidential information adhere to the requirements of U.S. law. This is achieved through a motion to quash, and such a motion may be made with respect to subpoenas issued by the government in its official actions. *See* Fed. R. Civ. P. 45(c); Fed. R. Crim. P. 17. Motions to quash government subpoenas are not uncommon. Similarly, the current body of U.S. civil rights law is predicated upon the ability of private actors to challenge governmental determinations that any acts taken "under color of law" comport with the Constitution and U.S. law. *See generally* 42 U.S.C. § 1983.

3. ***Assume a carrier is asked to assist with an intelligence program authorized by the President and is advised in writing that it has been determined to be lawful by Attorney General of the United States. What do you think a carrier in that position should do?***

   - ***If you believe that that the carrier should second-guess the government and potentially refuse, how do you address the fact that the carrier likely would not know enough about the underlying circumstances and operations of any program to make informed judgments about its propriety and legality?***

52426.001

- ***If the carrier interposes itself into the decision-making process, isn't there a significant risk that the government's terrorist-fighting capabilities will be degraded?***

- ***At a minimum, won't there be unpredictable delay, which could jeopardize our national security?***

A: Carriers should operate under a presumption that such a request is valid and make preparations to assist, but also forward the request immediately to in-house legal counsel for the green light. Counsel is responsible for corporate compliance with all laws including FISA, and should have mechanisms in place to deal with such national security requests expeditiously. Counsel should determine what laws apply and whether a particular request complies with statutory procedures for surveillance that would otherwise constitute unreasonable search/seizure of personal information on U.S. citizens.

If current FISA law requires either a Court Order or a certification by the Attorney General that the request complies with FISA, then the carrier should certainly expect to see such a document. If it does not, it would be appropriate to immediately contact the official requesting assistance to ask for further explanation. If none is forthcoming, we would expect counsel to advise against compliance with the request. The carrier should certainly not interpose itself into the federal government's decision-making process, but rather merely indicate whether it will or will not provide the requested surveillance, and if not, why not.

We would also expect corporate counsel to base its decision squarely on FISA law, and separate from any extraneous pending political, legal regulatory or policy issues in which the company may be involved.

Both the RESTORE Act passed by the House, and S. 2248 prescribe special procedures for emergency situations that allow immediate carrier compliance with emergency requests for wiretaps without delay, pending production of the appropriate legal documentation within 7 days.

4. ***Why do you believe it's a good thing for the country to expose classified intelligence activities through court proceedings? Doesn't this give our adversaries valuable information about our capabilities?***

A: As indicated by our testimony, we do not think this would be a good thing. Proceedings could be held *in camera* and the scope of discovery could be limited as not to expose sensitive information. If the court deems the case can't go forward on account of the State Secrets Privilege, then the cases will not proceed. In the past the courts have proven that they can adjudicate successfully on

52426.002

sensitive matters, and we should assume the same about the NSA wiretapping cases.

5. ***Do you believe it is appropriate for state public utility regulators to be investigating federal intelligence activities? Can you cite any other precedent for that kind of activity?***

A: State public utility commissions should not investigate federal intelligence activities. However, these agencies do have a concurrent jurisdiction with the FCC in terms of the security of telephone networks. PUCs have a fiduciary responsibility to the customers of regulated utilities and must not acquiesce to illegal wiretapping of those consumers or choose to ignore complaints regarding such activity by the regulated entities.

In the area of Communications Assistance for Law Enforcement (CALEA) wiretaps, PUCs can and do support carriers' expectations that proper legal procedures will be followed by federal law enforcement officials seeking wiretaps. Similarly, the PUCs expect carriers to observe procedures to protect subscriber privacy while delivering wiretap information to state and local law enforcement.

52426.003

December 2, 2007

Memorandum
To: Interested Parties
From Morton H. Halperin
Open Society Policy Center
Re: Service Provider Immunity Issues

SUMMARY: The arguments presented for providing retroactive immunity to the service providers who have been sued for alleged cooperation with the Bush Administration in conducting warrantless surveillance do not hold up under analysis. If Congress wants to facilitate the companies being able to defense themselves in court it should provide in the FISA legislation that the state secrets privilege cannot prevent a service provider from informing the court that it was told that the President approved the program and that the Attorney General had determined that it was lawful. If Congress does grant any relief to the service providers it should make clear, as the SSCI report does, that it views this as a one time act and insist that the service providers publicly commit that they will in the future cooperate with the government only when presented with a FISA court warrant or a certification that a warrant is not required under a specific provision of FISA.

INTRODUCTION

In order to understand the arguments presented for immunity it is important to consider the history which led Congress to enact FISA and to understand the rules which the law establishes for the service providers.

In the wake of Watergate and the related intelligence scandals, Congress was confronted with a parade of abuses in a number of areas including warrantless electronic surveillance. In the filed of international communications the Congress learned that in a number of situations the FBI, the CIA< and the National Security Agency (NSA) had cooperated with successive Presidents in acquiring information on people not even suspected of violating any laws. NSA had acquired all telegrams entering and leaving the United States. The Nixon Administration had wiretapped government officials and members of the press. The Kennedy Administration had wiretapped steel company executives. The FBI had wiretapped leaders of the civil rights and anti-war movements and on and on.

In each case, the phone company (then there was only one – AT&T) cooperated based on its belief that it had a common law obligation to do so in the absence of legislation and should not second-guess the President. Facing lawsuits and others and public controversy, AT&T sought clear guidance from the Congress. Congress acted on the belief that the only way to prevent future abuses was to legislate clear rules that would take the place of the common law obligation to aid the government when requested and immunity for doing so.

52426.004

AT&T received the clarity that it sought and deserved. FISA spelled out clearly that if AT&T received a copy of a warrant or a certification specified in FISA it was authorized to cooperate with a wiretap request. If it did not receive authorization by means outlined in FISA, it was to refuse to cooperate. If it violated these rules it would to be subject to state and federal civil and criminal penalties for assisting in the unlawful acquisition of electronic communications and open to lawsuits from subscribers whose rights it violated..

Regrettably, some service providers confronted by Bush Administration demands after 9/11 (and perhaps even before that date) failed to live up to their legal obligations as well as their responsibilities to their shareholders and to service subscribers. Told that the President had authorized the surveillance and that the Attorney General had determined that it was lawful, these service providers cooperated despite the fact that the requests violated the FISA rules by which they were legally bound.

Now faced with lawsuits by service subscribers, whose rights these companies failed to protect, the service providers are asking Congress to grant them immunity. The administration is strongly supporting this request. Indeed, the President warns that he will veto any legislation that does not provide retroactive immunity to service providers.

ARGUMENTS PRESENTED FOR GRANTING IMMUNITY

Four arguments for why the Congress should provide retroactive immunity are presented by the Administration and by advocates for the service providers. Two (the claim of common law immunity and the fear that classified information will inevitably been released) are without merit. The third (to encourage future cooperation outside of FISA) is in fact the strongest reason **not** to provide the immunity. Although the fourth (permitting the companies to defense themselves in court) has some validity, the problem it raises can be addressed by the Congress without undermining the rights of those whose telephone calls and emails were unlawfully provided to the government.

Common Law Immunity

The Bush Administration is arguing that the service providers who helped it conduct warrantless surveillance of Americans since 9/11 in violation of the Foreign Intelligence Surveillance Act (FISA) should be granted immunity based on the common law principle that a private citizen should cooperate when asked to do so by a law enforcement principle. This principle may well have justified immunity for the phone companies before FISA was enacted. (AT&T in fact prevailed when sued for pre-FISA wiretaps on precisely those grounds in several cases including one brought by me and my family) However, Congress has the power to change common law obligations by legislation, and that is precisely what Congress did when it enacted FISA in 1978.

Congress told the service providers precisely when they were to cooperate and provided immunity in those circumstances. The companies were well aware of FISA and its

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00064 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.005

obligations and cannot now claim any common law immunity. Indeed, the District Court judge hearing the consolidated cases in California fully considered this claim by AT&T and dismissed it on the merits finding that FISA replaced the common law principle. AT&T has not appealed this ruling but this has not stop its supporters from pressing this argument as if it were unassailable without informing the Congress that it had been rejected by the judge hearing the consolidated cases.

Threat of Release of Classified Information

The second argument is equally without merit. Allowing the lawsuits to go forward, it is argued, makes it likely that information that merits protection will be released inadvertently. There may have been a very few occasions in cases not related to electronic surveillance when a private party may have inadvertently been provided with information that the government intended to keep secret.. However, that happens much less often in federal courts than does the release of information by the Executive branch or by the Congress either inadvertently or by design. Moreover, Congress has provided for the use of classified information in a variety of legal situations and the federal courts now have procedures for storing, protecting, and using such information that work well in a variety of contexts. No classified information has leaked from the many cases challenging this electronic surveillance program. Most of the cases filed against the service providers have now been consolidated in a single court in California, which has shown that it is fully capable of protecting secrets. Moreover, no one proposes to end the many lawsuits against the *government,* so whatever risk there is, if any, will persist even if the cases against the service providers are ended.

Encouraging Service Provider Cooperation Outside of FISA in the Future

The third argument presented for providing retroactive immunity is, in fact, the strongest argument for **not** granting that immunity. The administration argues that if the service providers fail to get immunity they will be reluctant to cooperate in the future with requests from the government. By this the administration can only mean that service providers will hesitate to cooperate when they receive requests from the government which do not follow the procedures laid out in the law. There is no reason to fear that the service providers will refuse to cooperate when the law requires them to do so. The statute as written provides very clear guidelines for determining if a request to cooperate is lawful and it provides both penalties for refusing to provide assistance in such cases (if the FISA court affirms the request and directs cooperation) and an assurance of immunity if assistance is provided pursuant to the requirements of FISA.

Thus, the actual fear is that, if immunity is not granted, service providers will refuse to cooperate if once again confronted with a demand that they provide assistance outside of the law. In those circumstances, we want the service providers to send the administration to the Congress and to refuse to cooperate unless Congress authorizes the surveillance. **The greatest danger of granting immunity is that it will encourage future lawless conduct.**

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00065 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.006

It is true that we cannot be certain that Congress will anticipate all possible contingencies and always provide in advance the necessary authority to gather foreign intelligence information. Congress sought to deal with this danger in 1978 by providing that in the event of a declaration of war the government could conduct warrantless electronic surveillance for up to 15 days. A new version of such a provision might provide that if the President publicly declares a national emergency requiring the conduct of surveillance outside of FISA to deal with an international terrorism threat, he can conduct warrantless surveillance for up to 60 days. If the President informed a service provider that he was acting under this authority, the company would have the obligation to cooperate and the assurance of immunity for that period. Before the 60 days were up, Congress would no doubt provide the necessary authority in a manner consistent with the Fourth Amendment.

Giving the Service Providers Their Day in Court

The final argument for retroactive immunity, one made more often by the service providers than by the government, is that it is unfair to put them in a position where they cannot defend themselves because the government refuses to let them make public the requests or demands from the government that led them to cooperate. The implication is that a court would be likely to dismiss the complaint against them if it could review the certifications it received from the government. On its face, this claim would not seem to have any merit. FISA sets out clear obligations for the service providers and does not seem to leave any room for a good faith defense. Nonetheless, the service providers are entitled to put forward this defense and should be able to present to the court the certification they received from the government and their explanation of why they believe it compelled them or permitted them to cooperate.

The Senate Intelligence Committee has now made public the fact that service providers were given certifications every six months which said that the President had authorized the program and that the Attorney General had determined the program to be lawful.

In the lawsuits challenging the surveillance, the government has intervened and asserted what is known as the "state secrets privilege." The court hearing the consolidated cases has ruled that the certifications are not covered by the privilege and has ordered them disclosed. The government has appealed this ruling.

It is possible that the government will prevail in the appeal. If Congress wants to insure that the service providers can present this defense to the court, it could include in the pending FISA legislation a provision stating that those portions of the certifications provided to the service providers in which they are told that the President authorized the program and that the Attorney General had determined it to be lawful are not covered by the privilege.

Two objections will be raised. The first is that Congress does not have the power to do this. There is no question that in general Congress can alter common law privileges by legislation and it has often done so. The Bush Administration has argued in its briefs that

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00066 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.007

the state secrets privilege is "constitutionally based" and that Congress cannot waive the privilege as least for some categories of information, including those related to electronic surveillance. I believe that Congress can waive the privilege at least for the specific information that it has already made public and that this information should be sufficient to permit the service providers to present their good faith defense in court.

A second objection is that revealing which service providers were asked to cooperate and which did cooperate would reveal intelligence sources and methods. The court hearing the consolidated cases has already rejected this argument at least as to AT&T. It is very hard to understand how now revealing which service providers said yes and which said no to a now abandoned program can be of any value to a terrorist group. However, if this fact does need to be kept secret, the legislation could permit a service provider to inform the court in secret as to whether it cooperated. The court could then dismiss the complaint against a company if it found sufficient cause to do so without revealing whether it cooperated or not.

This approach would enable the service providers to raise their good faith defense, but it would not, and should not, insure that the case against them would be dismissed. The court might well find, as it should, that the service providers were obliged to follow the law and that the law left no room for a defense that they were doing what the President asked them to do.

In any case, until and unless a higher court reverses the finding that the privilege does not apply to this information and then goes on to determine that Congress cannot alter the privilege, Congress need do no more to permit the service providers to have their day in court.

The SSCI Approach to Retroactive Immunity

The Senate Select Committee on Intelligence (SCCI) version of the FISA bill as reported to the Senate goes much further. It accepts the need to keep the certifications secret and assumes that the service providers should be free of liability if they acted in good faith. Nonetheless, the Committee's rationale for providing this relief is fundamentally at odds with that of the administration and raises fewer concerns. Here is what it says:

> On the basis of the representations in the communications to providers, the Committee concluded that the providers, in the unique historical circumstances of the aftermath of September 11, 2001, had a good faith basis for responding to the requests for assistance they received. Section 202 makes no assessment about the legality of the President's program. It simply recognizes that, in the specific historical circumstances here, if the private sector relied on written representations that high-level Government officials had assessed the program to be legal, they acted in good faith and should be entitled to protection from civil suit.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00067 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.008

The Committee Report says plainly this is intended to be a "one time response" and the Committee clearly intends that in the future the service providers should permit access to communications only pursuant to specific provisions of FISA.

The Committee Report does not explain either why the committee believes that the service providers should be free of liability if they acted in good faith. Nor does it explain why the legislation directs the court to dismiss a service provider if the administration provides the specified certification rather than permitting a court to determine if a dismissal is justified. .

As I have already stated, I do not believe the case has been made for this approach. However, if this approach were to be considered, one would need assurances, thus far lacking, that the service providers themselves understand and accept this rationale for a one time immunity. Congress should insist that retroactive immunity would be available only to a service provider that has provided public assurances in writing to the Congress, to its shareholders, and its customers that in the future it will provide access to the communications of its customers only if it receives a court order or a certification of the form specified in the Senate Intelligence Committee bill. To be eligible for immunity or any other form of relief, such as substitution, a corporation should commit that, if confronted with any request or demand of the government for cooperation outside of FISA, it will refer to its public commitment, refuse to cooperate, and send the intelligence community to the Congress.

Conclusion

Although the retroactive immunity issue has gotten much of the public attention, it is far less important then many other issues that Congress is debating as it enacts amendments to FISA. In the end, it is critical that Congress adopt procedures for foreign intelligence surveillance that protect the privacy interests of all Americans and the Fourth Amendment rights of all persons in the United States. It is not yet clear that the legislation will do that. If it does, then the most important issue concerning the service providers would be to insure that in the future they cooperate with the government only pursuant to those procedures.

Morton H. Halperin is the Executive Director of the Open Society Policy Center and a Senior Fellow at the Center for American Progress. His phone was illegally wiretapped at the direction of the Nixon Administration from 1969-1971.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00068 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.009

November 27, 2007

Via messenger and email delivery

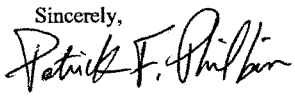
The Honorable Patrick J. Leahy
Chairman, Committee on the Judiciary
United States Senate Judiciary Committee
224 Dirksen Senate Office Building
Washington, D.C. 20510
Attention: Jennifer Price, Hearing Clerk

re: October 31, 2007 hearing re "FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability"

Dear Chairman Leahy:

Enclosed please find my answers to the questions for the record from Senator Brownback. Please let me know if I can be of further service.

Sincerely,



Patrick F. Philbin

Answers of Patrick F. Philbin to
Questions for the Record from Senator Brownback

1. Is a court order always required for a telecom carrier to furnish customer information or assistance to U.S. intelligence?

Answer: No, a court order is not always required. Several statutory provisions provide express authority for telecom carriers to furnish customer information or assistance to the government without the requirement of a court order. To give just a few examples, the FBI can obtain customer information through a National Security Letter under 18 U.S.C. § 2709; carriers can provide customer information in an emergency situation under 18 U.S.C. §§ 2702(b) and (c); the Attorney General can initiate coverage under the emergency provisions of FISA before obtaining a court order; and some law enforcement agencies have administrative subpoena authority that would permit them to obtain customer information under certain circumstances.

2. Some, including some members of this Committee, have suggested that telcos have an independent obligation to evaluate the underlying legality of an intelligence-gathering program and act as a further check on Executive decision-making in this area.

– Is this generally how the law is or has been structured to operate?

– In most circumstances, would a private company know enough about the underlying circumstances and operations to make informed judgments about legality?

– What are the implications to the country's terrorist-fighting capabilities of having private companies, which do not have all the facts, second-guessing the government's intelligence agencies?

Answer: The law has not generally been structured to require communications companies to conduct an independent review of the intelligence activities they are asked to support. In a run of the mill case concerning a FISA order or a title III warrant, a carrier likely has some obligation to review the materials it is presented (e.g., the order from the FISA court) to ensure they are not facially defective. That is not, however, the scenario being addressed here.

Communications carriers are not generally expected to conduct an independent review of the legality of an intelligence program they are asked to support. Conducting a complete evaluation of such issues would require access to classified information that is not available to the communications carriers. Moreover, having communications carriers conduct their own investigations and legal reviews into intelligence activities would create an element of delay that would be detrimental to securing swift access for the government to critical intelligence. Instead of that process, when carriers are assured that a program has been examined at the highest levels of the executive branch and found to be lawful, they should be able to rely on that assessment from the government.

52426.011

3. You and some of your colleagues developed serious reservations about the legal basis for at least some of the NSA's post-9/11 counterterrorism surveillance activities, and this led to the famous confrontation in John Ashcroft's hospital room. Shouldn't the carriers have been expected to make the same kinds of objections you did? Why not?

Answer: First, let me caution that in his public testimony, former Deputy Attorney General Comey did not tie the hospital room scene that he described to any particular intelligence activity, and my answer should not be taken as confirming or denying the connection of that scene to any particular intelligence program.

In any event, carriers should not be expected to raise the same kind of concerns. When they have been told that a program has been reviewed for legality at the highest levels of the Executive Branch, they should be able to rely on that representation. In addition, as a general matter, telecommunications carriers are simply not well-positioned to second-guess government decisions regarding the propriety or legality of intelligence activities. The legal questions involved in such matters are highly specialized, extremely difficult, often involve difficult constitutional questions of separation of powers and are not readily susceptible for analysis by lawyers at a company whose primary concern is providing communications service to the public. Answering the questions properly, moreover, can require detailed knowledge of how the particular intelligence activity fits into a broader picture and the threat it is designed to counter. We should not adopt policies that give private corporations incentives to demand detailed information from the Executive and in essence to conduct their own mini-investigations into the propriety of intelligence operations the government wishes to conduct. I believe creating those incentives would be at cross-purposes with the government's need for expedition in gathering critical intelligence in the midst of an ongoing war.

4. If companies that helped protect the country after 9/11 are forced to contend with this litigation firestorm, the public relations difficulties, the litigation costs and operations disruptions, as well as potentially ruinous liability, isn't their only rational response to be more reluctant in the future to help the government? Wouldn't that dramatically undercut the country's terrorist-fighting capabilities?

Answer: I believe that permitting the suits to continue, with all the attendant effects you have described, would provide incentives for carriers to be far more reluctant in the future to aid the government in intelligence activities. As a matter of policy, that is precisely the wrong incentive for the government to create. One of our Nation's greatest strategic assets in the continuing conflict with al Qaeda is the private sector and the information it can help provide to the intelligence community. Particularly in this war with an enemy that attacks by stealth, intelligence is vital for success. If the lawsuits against carriers are permitted to proceed, it is likely that, in the future, private sector corporations will prove much more reluctant to provide assistance to the government swiftly and willingly, and critical time in obtaining information will be lost. I agree fully with the conclusion in the report accompanying the bill from the Select Committee on Intelligence: "The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation." S. Rep. 110-209, at 11.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00071 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.012

5. One particular concern of mine is that allowing these lawsuits to continue risks the disclosure of national security secrets that must be kept from public view if our intelligence agencies are to be able to protect us effectively. Do you share that concern?

Answer: Yes, I do share that concern. As the suits progress, they will inevitably risk disclosure of intelligence sources and methods that will damage the national security of the United States in the midst of our continuing struggle with al Qaeda. The assertion of state secrets privilege is not a cure-all for protecting national security information. The privilege has already been rejected by one district court judge in one case, and if it were a swift and effective means of shutting down litigation that risked disclosing secrets, the cases consolidated in California would not still be pending almost two years after they were filed. The longer the suits proceed, the more details concerning the ways the intelligence community may seek information from the Nation's telecommunications infrastructure will leak. Our enemies are far from stupid. As such information trickles out, they will adapt their communications security to thwart our surveillance measures, and valuable intelligence will be lost.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00072 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.013

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

January 16, 2009

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Please find enclosed responses to questions arising from the appearance of then-Assistant Attorney General Kenneth Wainstein before the Committee on October 31, 2007, at a hearing entitled "FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability." We apologize for the length of time necessary to prepare these responses. We hope that this information is of assistance to the Committee. Please do not hesitate to call upon us if we may be of additional assistance.

The Office of Management and Budget advises us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Keith A. Nelson
Principal Deputy Assistant Attorney General

Enclosure

cc: The Honorable Arlen Specter
Ranking Minority Member

Committee on the Judiciary
United States Senate

"FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability"

October 31, 2007

Responses of
the Department of Justice
to Questions Posed to
then-Assistant Attorney General
Kenneth L. Wainstein

Questions from Senator Leahy:

1. **Both the Protect America Act and the Senate Intelligence Committee bill would change the definition in FISA of "electronic surveillance" to say that it does not include surveillance of a target overseas, even if that target is communicating with someone in the United States.**

   First, this is nonsensical – this clearly is electronic surveillance and to have a statute say that black is white is a bad practice. This change would also have consequences for other parts of the statute that use that definition. For example, there is a question about whether it renders inapplicable the civil and criminal liability provisions contained in FISA because those provisions are triggered by unauthorized "electronic surveillance."

   Most importantly – it seems entirely unnecessary. The next part of the legislation would set up a new procedure for conducting the surveillance the government wants. There is no need to except it from the definition.

   Q: Do you agree that if the statute sets up an alternative procedure to conduct the surveillance in the legislation, there is nothing in changing the definition that would add to the government's authority? If not, please explain in as much detail as possible what the definitional change accomplishes.

Answer: We are grateful that Congress passed and the President signed the FISA Amendments Act of 2008 (FAA), Pub. L. No. 110-261, enacted on July 10, 2008. That Act did not contain a carve-out of the definition of electronic surveillance analogous to that contained in the Protect America Act (PAA).

52426.015

Immunity – Takings Issue

2. Retroactive immunity would strip away the rights of plaintiffs in those lawsuits to pursue on-going litigation that alleges violations of constitutional rights.

Q: Are there constitutional problems with doing this? Is it a "Taking" that violates the 5th amendment?

ANSWER: No. We do not see any constitutional problems with the immunity provision, and it would not constitute a taking under the Fifth Amendment.

If there are no constitutional problems, can you point us to precedent where Congress has stepped in to quash on-going constitutional litigation?

ANSWER: The vast majority of the claims to which the immunity provisions would apply sound in tort and are not based on the Constitution. Congress has passed legislation that effectively ended litigation against private parties in the past. For instance, in 2005, Congress passed the Protection of Lawful Commerce in Arms Act (PLCAA) to protect the firearms industry from liability under state tort law (both statutory and common law). Like the recently enacted legislation, the PLCAA applied to pending cases. The Justice Department has successfully defended the statute in district court litigation involving tort law and a number of those cases are currently on appeal.

An exemplar case is *District of Columbia, et al. v. Beretta U.S.A. Corp.*, Nos. 06-CV-721, 06-CV-757 at 3 (D.C. Court of Appeals, January 10, 2008), in which individual plaintiffs and the District of Columbia sued various gun manufacturers, importers, and distributors of firearms, alleging, among other things, negligence, and creation of a public nuisance. The appellate court affirmed the trial court and held, *inter alia*, that the PLCAA does not violate separation of powers principles or due process principles embodied in the Fifth Amendment, or constitute a taking under the Fifth Amendment. *Id.* at 2.

Another example is *Ileto v. Glock*, 421 F. Supp. 2d 1274 (C.D. Cal. 2006). In *Ileto*, shooting victims and their family members brought an action in state court against the manufacturers, distributors, and dealers of firearms used and possessed by an assailant at the time of an assault, alleging survival and wrongful death claims and public nuisance and negligence claims. *Id.* at 1277-79. Following removal to federal district court, the manufacturer moved to dismiss. *Id.* On remand, the district court held, *inter alia*, that the victims' causes of action against gun manufacturer and distributor did not constitute vested property interests; retroactive provision of the PLCAA did not violate shooting victims' right to due process; PLCAA did not violate the constitutional prohibition on bills of attainder; and PLCAA did not violate equal protection under the Fifth Amendment. *Id.* at 1298-1304.

We believe the abrogation of similar claims against private parties based on alleged constitutional violations would be constitutional as well. In any event, the plaintiffs in the

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00075 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.016

litigation at issue face serious difficulties in successfully asserting that private parties have violated constitutional provisions that apply generally only to the conduct of the government.

If there are constitutional problems, do the retroactive immunity provisions contained in the Senate Intelligence bill address them?

ANSWER: As explained above, there are no constitutional problems with the immunity provisions.

3. **The Senate Intelligence Committee bill would require the Government to submit targeting and minimization procedures to the FISA Court for the court's review, but it would not require an up-front order from the FISA Court. The companies assisting with the surveillance would get their direction from the Attorney General and the DNI, not the Court.**

   Q: With the Senate Intelligence Committee bill, please describe your understanding of what power the FISA Court would have to stop the Government from acquiring communications if it determines that the targeting or minimization procedures are flawed?

Answer: Absent exigent circumstances, section 702 of FISA, as added by the FISA Amendments Act of 2008, requires the Government to obtain the approval of the Foreign Intelligence Surveillance Court (FISC) of its foreign targeting and minimization procedures before targeting persons reasonably believed to be located outside the United States in order to acquire foreign intelligence under the provisions of the statute. *See* 50 U.S.C. § 1881a.

4. **The Report accompanying the Senate Intelligence Committee's legislation notes with respect to the "Terrorist Surveillance Program" that the Executive Branch provided the service providers with letters at regular intervals stating that the activities they were being asked to assist the government with had been deemed lawful by the Attorney General. The Report says this is true for all the letters except one. One letter stated that the Counsel to the President, not the Attorney General, had deemed the activities to be lawful.**

   Q: Even if you argue that the companies acted legally in compliance with FISA through most of this time, you cannot make that argument with respect to the period of time when Mr. Gonzales – then White House Counsel – approved the letters, can you?

Answer: As the Senate Select Committee on Intelligence recognized, "if the private sector relied on written representations that high-level Government officials had assessed the program to be legal, they acted in good faith and should be entitled to protection from civil suit." S. Rep. No. 110-209 at 11.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00076 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.017

Q: Given that the service providers provided assistance without regard for the statutory requirements for certification laid out in FISA and Title III, if we give them immunity now, how can we assure ourselves that they will follow the statutory requirements of FISA in the future and not just accept any written certification that the Administration gives them?

Answer: In January 2007, the Attorney General announced that, as a result of the orders granted by the Foreign Intelligence Surveillance Court on January 10, 2007, any electronic surveillance that was occurring as part of the Terrorist Surveillance Program ("TSP") would be conducted subject to the approval of the FISC. In addition, as you know, the Protect America Act helped close critical intelligence gaps. FISA, the Protect America Act, and the FISA Amendments Act provide for statutory protection for providers that comply with government requests for assistance under their provisions. The immunity provision passed by the Congress is a one-time grant of retroactive immunity for a discrete set of activities designed to "detect and prevent the next terrorist attack" after September 11th. S. Rep. No. 110-209 at 11. As the Intelligence Committee stated, the immunity "should be understood by the Executive branch and providers as a one-time response to an unparalleled national experience in the midst of which representations were made that assistance to the Government was authorized and lawful." *Id.* at 12.

5. **You stated more than once in your testimony that if any litigation should occur, it should be directed against the government, not the communications carriers who assisted the government. However, when I asked you how this would be done in light of the government's blanket assertions of state secrets, you responded, "there are many investigations going on right now about the propriety of what was done or not done under the Terrorist Surveillance Program. So in terms of accountability, if there is wrongdoing, that wrongdoing is being ferreted out in ways, very traditional ways, other than litigation."**

Q: Please specify what particular avenues, other than litigation, you are suggesting we use to hold any wrongdoers involved in this matter accountable?

Answer: As you are aware, there are ongoing investigations of the Terrorist Surveillance Program by various government entities, including the Department of Justice's Inspector General and the Department's Office of Professional Responsibility. The FISA Amendments Act of 2008 requires the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and any other element of the intelligence community that participated in the President's Surveillance Program to complete a comprehensive review of those Departments' and Agencies' activities under the Program by July 10, 2009. *See* FISA Amendments Act of 2008 § 301(b)(1). These entities, among others, are authorized to make recommendations to the Attorney General and other senior government officials to address any problems that their reviews may uncover. In addition, as you know, the House and Senate Judiciary and Intelligence Committees have held extensive oversight hearings in this area.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00077 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.018

Questions from Senator Feingold

1. **The Senate Intelligence Committee bill provides new authority for targeting individuals 'reasonably' believed to be located overseas. That determination of the target's physical location prevents warrantless wiretapping of Americans inside the United States, so it is critical that the government establish effective procedures to make sure it only uses this authority to target people overseas. Under the bill, the government starts using its targeting procedures before submitting them to the court for approval. If the court ultimately rejects those procedures, and determines that they are not reasonably designed to ensure that only overseas targets are wiretapped using these new authorities, what does the bill say would happen to all the communications involving U.S. persons that were acquired using the unlawful procedures before the court rejected them?**

Answer: Absent exigent circumstances, section 702 of FISA, as added by the FISA Amendments Act of 2008, requires the Government to obtain FISC approval of its foreign targeting and minimization procedures before targeting persons reasonably believed to be located outside the United States in order to acquire foreign intelligence under the provisions of the statute. *See* 50 U.S.C. § 1881a.

2. **Does the Justice Department believe 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 unlawful behavior?**

Answer: We do not believe that litigation regarding any assistance provided by telecommunications providers to the Government in the aftermath of the September 11th attacks is an appropriate enforcement mechanism where the companies acted pursuant to requests or directives assuring them that the President had authorized the activities and that the activities had been found to be lawful. This is particularly true in light of the harm to the national security that could result from disclosures of classified information during litigation and the deterrent effect that such litigation may have on private partners that are asked to assist with lawful Government requests in the future.

3. **The Intelligence Committee Report on the FISA bill declassified for the first time the fact that after September 11, 2001, the administration provided letters to communications service providers seeking their assistance with communications intelligence activities authorized by the President. What is the Justice Department's position as to whether those letters comply with the statutory immunity provision in existing law, which is in Section 2511(2)(a) of Title 18?**

Answer: The FISA Amendments Act of 2008 provides liability protection to companies that either did not act or received either court orders, statutory certifications under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, certain statutory directives, or certain written requests or

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00078 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.019

directives from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) indicating that the activity was authorized by the President and determined to be lawful. The question of whether the letters provided to the telecommunication carriers constituted section 2511 certifications therefore is not dispositive. At this time, the Department cannot comment publicly on that question in light of the ongoing litigation concerning that very issue.

4. **Five weeks ago, I asked DNI McConnell whether the administration could provide this Committee with information about how much U.S. person information is looked at and how much is disseminated, under the new authorities provided in the Protect America Act. He told me that the information was already being compiled and should be ready in a matter of weeks. As far as I am aware, that information has not yet been provided. When will the Judiciary Committee get that information?**

Answer: The Department of Justice does not have the information you seek.

5. **The Senate Intelligence Committee bill, like the Protect America Act, amends FISA's definition of "electronic surveillance." The consequences of that change are unclear. Does the Administration believe that it is necessary to amend that key definition? Would the legislation have the same effect if it added new authorities but allowed the new definition of electronic surveillance in the Protect America Act to expire?**

Answer: The FAA did not contain a carve-out of the definition of electronic surveillance analogous to that contained in the Protect America Act.

6. **The Intelligence Committee bill permits the executive branch to begin surveillance based on its own procedures, and requires that they be submitted to the court only after the fact. What would be the harm in having the court review and approve the procedures prior to using them, with a provision for going forward without prior judicial review in an emergency?**

Answer: Absent exigent circumstances, section 702 of FISA, as added by the FISA Amendments Act of 2008, requires the Government to obtain FISC approval of its foreign targeting and minimization procedures before targeting persons reasonably believed to be located outside the United States in order to acquire foreign intelligence under the provisions of the statute. *See* 50 U.S.C. § 1881a.

7. **Do you agree that there is 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?**

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00079 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.020

Answer: In either case, under the PAA (or section 702 of FISA, as added by the FISA Amendments Act of 2008), we would have targeted the foreign intelligence target overseas. Assuming that we are effectively collecting all communications to or from the foreign intelligence target located outside the United States, from a privacy standpoint it should not make a difference where we conduct the acquisition.

Absent exigent circumstances, section 702 of FISA, as added by the FISA Amendments Act of 2008, requires the Government to obtain FISC approval of its foreign targeting and minimization procedures before targeting persons reasonably believed to be located outside the United States in order to acquire foreign intelligence under the provisions of the statute. *See* 50 U.S.C. § 1881a. These procedures ensure that the privacy interests of United States persons are protected with respect to acquisitions under that section. Furthermore, section 702 also establishes five related limitations on the authority granted by that section. The first prohibits the use of the new authority to target intentionally any person within the United States; the second provides that the authority may not be used to conduct "reverse targeting," the intentional targeting of a person reasonably believed to be outside the United States if the purpose of the acquisition is to target a person reasonably believed to be in the United States; the third bars the intentional targeting of a United States person reasonably believed to be outside the United States; the fourth limitation goes beyond targeting (the object of the first three limitations) and prohibits the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and the fifth establishes that acquisitions authorized under the section shall be conducted in a manner consistent with the Fourth Amendment to the U.S. Constitution. 50 U.S.C. § 1881a.

8. **Do the new authorities provided in the Intelligence Committee-passed FISA bill authorize the acquisition, from inside the United States, of any foreign-to-foreign communications in which a target is not a communicant? Do they authorize such acquisition of any foreign-to-domestic communications in which a target is not a communicant? Do they authorize such acquisition of any domestic-to-domestic communications in which a target is not a communicant?**

Answer: This answer cannot be provided in an unclassified setting.

9. **As defined in Section 2510(15) of Title 18, the term "electronic communication service" is quite broad, and covers "any service which provides to users thereof the ability to send or receive wire or electronic communications." Does the Department of Justice believe that Title I of the FISA bill reported by the Senate Select Committee on Intelligence, S. 2248, which applies to providers of electronic communication services as defined in Section 2510 of Title 18, covers libraries that provide Internet access to their patrons or places of business that provide their staff with Internet access?**

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00080 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.021

Answer: Whether a particular institution could qualify as an "electronic communications service provider" is a complicated legal question that depends on the facts and circumstances involved in each case. It is important to note, however, that if the target of intelligence collection is a person in the United States, FISA requires the Government to go to the Foreign Intelligence Surveillance Court for an order to conduct electronic surveillance of that target — under the same circumstances it would have before the Protect America Act passed. In the same way, section 702 of FISA, as added by the FISA Amendments Act of 2008, provides that the authority granted by that section cannot be used to intentionally target any person known at the time of the acquisition to be located in the United States. 50 U.S.C. § 1881a.

In addition, under the Protect America Act and the FAA, a recipient of a Government directive for assistance or information related to the acquisition of foreign intelligence information has the opportunity to contest that directive in court. *See* 50 U.S.C. § 1881a.

10. The Protect America Act contains a provision that permits communications service 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?

Answer: Section 4 of the Protect America Act provided that the Attorney General shall report to the Intelligence and Judiciary Committees on a semiannual basis, among other things, a "description of any incidents of non-compliance with a directive issued by the Attorney General and the Director of National Intelligence under section 105B, to include . . . incidents of noncompliance by a specified person to whom the Attorney General and Director of National Intelligence issue a directive." We have complied with this reporting requirement and have also committed to go beyond this statutory requirement and to share with the Intelligence and Judiciary Committees appropriately redacted documents related to any such challenges, consistent with the national security.

b. Will you commit to announcing, publicly, the fact that such a petition has been filed?

Answer: Due to concerns regarding the possible disclosure of classified information, the Department cannot commit to publicly stating whether or not such petitions have been filed. Communications intelligence activities are among the most highly classified intelligence activities undertaken by the Government. Our adversaries are intensely interested in information regarding our vital communications intelligence activities, including the nature, scope, and methods of those activities used to protect the country and our interests around the world. Armed with such information, they could modify their activities to evade detection by our intelligence community. Information pertaining to our use of the Protect America Act is, and

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00081 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.022

should be, appropriately classified to avoid such disclosures. Thus, while we can, consistent with the national security, report any such events to the Intelligence Committees and Judiciary Committees, the Department cannot commit to announcing such events publicly.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00082 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.023

Questions from Senator Kennedy:

1. **Thank you, Mr. Wainstein, for sharing your views on FISA with the members of this Committee. I regret that I was unable to attend the hearing in person. As the history of our surveillance laws teaches us, it's 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 authority they needed, and also build in checks and balances to prevent abuse of that authority. FISA proved that we do not have to choose between civil liberties and national security.

   Unfortunately, the Protect America Act was enacted this summer in a much less thoughtful process. It was negotiated in secret and at the last minute. The Administration issued dire threats that failure to enact the law before the August recess could lead to disaster. We need to correct that failure by engaging in a thorough, deliberative process before we enact more legislation.

   It is encouraging that the Administration has finally agreed to share documents with members of this Committee and the Senate Intelligence Committee on its warrantless surveillance program. We had requested these documents for many months, because they are clearly relevant to the Administration's arguments on FISA.

   But the Administration has not yet shared any documents with members of the House Judiciary or Intelligence Committees, whose new FISA bill it has criticized. This selective information-sharing is troubling because it suggests that the Administration will only work with those lawmakers who already agree with it.

Questions:

1. **Why won't the Administration share the documents on its warrantless surveillance program with the House Intelligence and Judiciary Committees? Aren't these committees equally important players in this legislative debate?**

Answer: The FISA Amendments Act of 2008 resulted from extensive exchanges of information, briefings, and consultations between Congress and the Executive Branch. In order to better inform the debate concerning liability protection, the Senate Intelligence and Judiciary Committees were provided with access to documents and other information relating to the President's Terrorist Surveillance Program.

2. **White House press secretary Dana Perino was recently asked why the Administration was willing to share documents with the Senate Intelligence Committee but not with any others. She said it was because the Intelligence**

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00083 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.024

Committee's leaders "showed a willingness" to grant amnesty to the telecommunications companies. "Because they were willing to do that," Ms. Perino said, "we were willing to show them some of the documents that they asked to see." Asked to clarify these disturbing comments several days later, a White House spokesman said that what the Administration did was "not exactly" a quid pro quo.

a. Do you stand by these descriptions of the Administration's behavior?

Answer: Please see the response to Question 1 above.

b. These documents contain information that is clearly relevant to our responsibilities as lawmakers. How can you defend a policy of sharing them only with the committees that agree with the White House's preferences?

Answer: Please see the response to Question 1 above.

2. This Administration has asserted a view of executive power that is breathtaking in its 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 here, the President defied clear statutory language.

Questions:

1. If Congress enacts a FISA bill, will the President accept that he is bound by it? In particular, if we pass a bill that gives the President less power to conduct surveillance than he is now exercising, will he comply with it?

Answer: Foreign intelligence surveillance must be conducted in accordance with the Constitution and laws of the United States. A duly enacted statute, FISA has been and continues to serve as the framework for conducting electronic surveillance in the United States of foreign powers and agents of foreign powers. The Protect America Act of 2007 avoided any potential conflict between FISA and the core Executive Branch function of protecting the United States from foreign threats because it provided a statutory mechanism for conducting critical foreign intelligence surveillance activities. The FISA Amendments Act of 2008 continues to provide this statutory authority.

2. If we do not extend the Protect America Act and do not pass any other new laws, will the Administration comply with FISA?

Answer: The FISA Amendments Act of 2008 achieves the objective of providing critical authorities needed by the Intelligence Community to protect the Nation.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00084 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.025

3. **Are any electronic surveillance programs currently being conducted outside the authority of FISA as amended by the Protect America Act?**

Answer: Since January 2007, electronic surveillance for foreign intelligence purposes has been conducted consistent with orders and authorizations under the Foreign Intelligence Surveillance Act, including as it was amended by the Protect America Act and the FAA.

4. **Do you agree that new legislation should reaffirm that FISA is the sole means by which the Executive branch can conduct electronic surveillance outside of the criminal context?**

Answer: The FISA Amendments Act of 2008, crafted through extensive bipartisan cooperation, amends Title I of FISA and provides a statement of exclusive means by which electronic surveillance and the interception of certain communications may be accomplished.

3. **As you know, the Administration is asking Congress to grant broad immunity for any past violations of the law by telecommunications companies that provided surveillance information. The Senate Intelligence Committee's bill grants this amnesty; the House Intelligence and Judiciary Committees' bill does not.**

I have yet to hear a single good argument in favor of amnesty for the telecoms, but there are many reasons to be against it. Under FISA, communications carriers already have immunity from liability if they act pursuant to a court warrant or a certification from the Attorney General. In this way, FISA protects carriers who follow the law, while enlisting their help in protecting Americans' rights and the integrity of our electronic surveillance laws.

The Administration's proposal for immunity will help shield illegal activities from public scrutiny, but it will do nothing to protect our security or liberty. Instead, it will deprive plaintiffs of their rightful day in court, send the message that violations of FISA can be ignored, and undermine an important structural safeguard of our surveillance laws.

It's especially disturbing that the Administration apparently encouraged communications companies to break the law, and that those companies apparently went along. It's wrong to allow the Executive Branch to pick and choose which laws it obeys, and to ask others to help it break the law.

Questions:

1. **Isn't it true that under FISA, companies that acted pursuant to a court order or an Attorney General certification already have immunity from liability?**

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00085 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.026

a. Is it fair to say, then, that none of the telecoms being sued had one of these two documents, because if they did, they would already be off the hook?

Answer: The FISA Amendments Act of 2008 provides liability protection to companies that either did not act or received either court orders, statutory certifications under section 2511(2)(a)(ii)(B) or 2709(b) of title 18, certain statutory directives, or certain written requests or directives from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) indicating that the activity was authorized by the President and determined to be lawful. Whether or not the telecommunication carriers acted pursuant to a court order or Attorney General certification therefore is not the only relevant question under the Act. In order to better inform the debate concerning liability protection, the Senate Intelligence and Judiciary Committees were provided with unprecedented access to documents and other information relating to the President's Terrorist Surveillance Program.

2. In your testimony, you suggested that it would be "unfair" to the telecommunications companies to let the lawsuits proceed. I found this argument most unconvincing. Telecommunications companies have clear duties under FISA, and they have highly sophisticated lawyers who deal with these issues all the time. It is precisely because fairness and justice are so important to the American system of government that we ask an independent branch—the judiciary—to resolve such legal disputes. There is nothing fair about Congress stepping into ongoing lawsuits to decree victory for one side.

a. If a company violated its clear duties and conducted illegal spying, doesn't fairness demand that it face the consequences?

Answer: After reviewing the relevant documents, and without identifying either the specific companies or the activities for which the companies provided assistance, the Senate Intelligence Committee concluded that the providers had acted in response to written requests or directives stating that the activities had been authorized by the President and had been determined to be lawful. Because the committee "concluded that the providers . . . had a good faith basis for responding to the requests for assistance they received," *id.* at 11, the committee concluded that the providers "should be entitled to protection from civil suit." *Id.* The committee's considered judgment reflects a principle in the common law that private citizens who respond, in good faith, to a request for assistance by public officials should not be held liable for their actions.

3. If Congress bails out 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?

Answer: The liability protection provisions of the FISA Amendments Act of 2008 do not set a bad precedent. The provisions are limited in scope and protect only those companies that either did not provide the alleged assistance, or acted pursuant to a court order, statutory directive or

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00086 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.027

certification, or a written directive or request from a high ranking government official indicating that the activity was authorized by the President and determined to be lawful.

The Senate Intelligence Committee concluded that the providers had acted in response to written requests or directives stating that the activities had been authorized by the President and had been determined to be lawful. S. Rep. No. 110-209 at 10. Because the committee "concluded that the providers . . . had a good faith basis for responding to the requests for assistance they received," *id.* at 11, the committee concluded that the providers "should be entitled to protection from civil suit." *Id.* The provision is a one-time grant of retroactive immunity for a discrete set of activities designed to "detect and prevent the next terrorist attack" after September 11th. *Id.* As the Intelligence Committee stated, the immunity "should be understood by the Executive branch and providers as a one-time response to an unparalleled national experience in the midst of which representations were made that assistance to the Government was authorized and lawful." *Id.* at 12.

We also believe that existing congressional oversight mechanisms are sufficient to help Congress be informed on intelligence activities.

4. **If your concern is that carriers not be bankrupted, would you support something more specific than complete amnesty—for example, a cap on damages?**

Answer: No.

   a. **If not, why not? Are you worried that courts will rule that the President's warrantless surveillance programs were illegal?**

Answer: No. The liability protection provided by the FISA Amendments Act of 2008 is designed to ensure that companies are not exposed to lengthy and costly litigation based on allegations that they assisted the United States in protecting the nation against terrorist attack—litigation which could deter private individuals and entities from helping the Government in vital counterterrorism efforts in the future. A cap on damages would not achieve the same goal. The lawsuits themselves discourage cooperation by telecommunications companies. Moreover, because a cap on damages would not end the litigation, it would not eliminate the risk to the national security caused by the possibility of disclosure of information in the context of alleged intelligence activities designed to detect and protect against terrorist attacks. Finally, as a bipartisan majority of Congress recognized in passing the FISA Amendments Act of 2008, liability protection is the just result for companies being sued only because they are believed to have assisted the Government in the aftermath of September 11th.

5. **As you know, the President has said he will veto any FISA bill that does not grant retroactive immunity. At the same time, he and the Director of National Intelligence have said that if Congress does not make major changes to FISA,**

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00087 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.028

American lives will be sacrificed. If we take him at his word, then, the President is willing to let Americans die on behalf of the phone companies

a. **That's hard to believe. So why does the President insist on amnesty for the phone companies as a precondition for any FISA reform?**

Answer: Liability protection is tied directly to our operational need to have an effective foreign intelligence collection system, and is thus an integral part of FISA modernization. Companies have been subject to lawsuits based on their alleged involvement in certain alleged intelligence activities, and such suits can be lengthy, costly, and unpredictable. Such litigation could deter private individuals and entities from helping the Government in vital counterterrorism efforts in the future, which would hurt the nation's security. As the Senate Intelligence Committee noted in its report on S. 2248, "electronic communication service providers play an important role in assisting intelligence officials in national security activities. Indeed, the intelligence community cannot obtain the intelligence it needs without assistance from these companies." S. Rep. No. 110-209 at 11. Because of the need for such cooperation in the future and the extent of the lawsuits that have been filed, that committee concluded that retroactive immunity was a necessity.

> Given the scope of the civil damages suits, and the current spotlight associated with providing any assistance to the intelligence community, the Committee was concerned that, without retroactive immunity, the private sector might be unwilling to cooperate with lawful Government requests in the future without unnecessary court involvement and protracted litigation. *The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation.*

Id. (emphasis added).

4. **As you know, the Senate Select Committee on Intelligence recently reported a FISA bill, the "FISA Amendments Act of 2007," which has now come to this Committee on sequential referral. This bill would make major revisions to our surveillance laws in a variety of areas.**

Although I appreciate the work of my colleagues on the Intelligence Committee in drafting this legislation, I have some concerns about their bill. For example:

- **As I have said, the bill provides amnesty to telecommunications companies that may have broken the law in cooperating with the Administration on illegal surveillance, even though they already have broad immunity under current FISA law.**

- **The Intelligence Committee's bill redefines "electronic surveillance" in a way that is unnecessary and may have unintended consequences.**

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00088 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.029

- **The bill does not fully close the loophole left open by the Protect America Act, allowing warrantless interception of purely domestic communications.**

- **The bill does not require an independent review and report on the Administration's warrantless eavesdropping.**

- **The bill purports to eliminate the "reverse targeting" of Americans, but does not actually contain language to do so. There is nothing analogous to the House bill on reverse targeting, which prohibits such surveillance if "a significant purpose" is targeting someone in the United States.**

- **Court review occurs only after-the-fact, with no consequences if the court rejects the government's targeting or minimization procedures.**

These are just a few of my concerns. But if I understand you correctly, you are generally supportive of the Intelligence Committee bill. Certainly, you seem to like it a lot more than the bill being considered by the House, which contains significantly greater protections for civil liberties.

Questions:

1. **My understanding is that you are in favor of the way the Intelligence Committee bill redefines "electronic surveillance." In his written testimony, Mort Halperin described this change as "Alice in Wonderland": "It says that the language in FISA, which defines 'electronic surveillance,' means not what it clearly says, but what the current bill says it says."**

    a. **Why should we change the definition of "electronic surveillance"? It's a central term in FISA, and I see no good reason to replace it and open the door to many unintended consequences.**

Answer: The FISA Amendments Act of 2008, enacted on July 10, 2008, did not contain a carve-out of the definition of electronic surveillance analogous to that contained in the Protect America Act.

    b. **Mort Halperin has recommended that we strike out the part of the Intelligence Committee bill that redefines "electronic surveillance," and then change the requirements for the certification to be given to the FISA court to read "the surveillance is targeted at persons reasonably believed to be located outside the United States." How would this change affect your understanding of the legislation?**

Answer: Please see the response to question 1.a. above.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00089 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.030

2. **Unlike the House bill, the Intelligence Committee bill does not require prior judicial authorization before surveillance begins. This is a major departure from how FISA has always worked. It raises serious civil-liberties concerns, and makes it very difficult for courts to cut off surveillance that is illegal under the law. As Mort Halperin has stated: "By definition, if there is no emergency, there is time to go to the court and there is no reason to allow the executive branch to begin a surveillance without first having court approval. Requiring as a matter of routine that court approval must come first will assure that the executive branch gives the matter the full consideration that it deserves before starting a surveillance which will lead to the acquisition of many communications of persons in the United States and Americans abroad. . . . I cannot imagine any public policy argument to the contrary once one concedes that the court needs to play a role and there is an exception for emergencies with ample time limits."**

   a. **How do you respond to Mr. Halperin's arguments?**

Answer: Absent exigent circumstances, section 702 of FISA, as added by the FISA Amendments Act of 2008, requires the Government to obtain FISC approval of its foreign targeting and minimization procedures before targeting persons reasonably believed to be located outside the United States in order to acquire foreign intelligence under the provisions of the statute. *See* 50 U.S.C. § 1881a.

   b. **Doesn't the abandonment of *before*-the-fact court review go against the basic promise of FISA that Americans will not have their communications acquired without a judge confirming that there is a legitimate reason to do so?**

Answer: Please see the response to question 2.a. above.

3. **If you agree that purely domestic-to-domestic communications should never be acquired without a court order, would you support changes to the bill that would make this point 100% clear? As I read the bill, this is not as clearly prohibited as it could be.**

Answer: FISA already requires a FISC order for the electronic surveillance of purely domestic-to-domestic communications, and section 702 of FISA, as added by the FISA Amendments Act of 2008, expressly prohibits the targeting of persons located in the United States under the authority provided in that section. *See* 50 U.S.C § 1881a.

4. **If you agree that warrantless "reverse targeting" of Americans should never be allowed, would you support language in the bill to prohibit its use if "a significant purpose" is targeting someone in the United States?**

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00090 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.031

Answer: Section 702 of FISA, added by the FISA Amendments Act, prohibits such "reverse targeting" and provides that an acquisition under that section "may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States." 50 U.S.C. § 1881a.

a. If not, why not? The House bill contains this provision, and it's a sensible way to address the very serious "reverse targeting" concerns that will make Americans afraid for their rights.

Answer: Please see the answer provided above.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00091 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.032

Questions from Senator Kyl:

An amendment that was added to this bill in the Intelligence Committee by Senator Wyden adds a section to FISA that requires U.S. agents to obtain a warrant to conduct *overseas* surveillance of national-security threats if that surveillance targets a U.S. person.

1. **Some advocates of this provision have described it as protecting the rights of U.S. citizens. The bill text, however, appears to cover "U.S. persons" – a category that FISA defines to even include U.S. green card holders. As I read the Wyden amendment, if a Pakistani national came to the United States as an adult for a few years, acquired a green card, and then returned to Pakistan and joined up with Al Qaeda, then under the Wyden amendment, this Pakistani national would be granted privacy rights under FISA that would bar the United States from monitoring his communications with the rest of Al Qaeda without first obtaining a warrant. Is that description accurate?**

Answer: The requirement set forth in Senator Wyden's amendment for prior court approval would extend to individuals with a valid status as lawful permanent residents (*i.e.*, green card holders). Section 704 of FISA, as added by the FISA Amendments Act of 2008, provides that no element of the intelligence community may intentionally target, for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes unless the Attorney General (or his designee) submits an application to the FISC and receives an order from the FISC approving that acquisition.

The term "United States person" includes "a citizen of the United States" or "an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8)." 50 U.S.C. § 1801(i). Thus, if an individual possessed valid and lawful permanent resident status, but was located outside the country, absent exigent circumstances, the FISA Amendments Act of 2008 requires prior court approval for certain acquisitions of foreign intelligence information targeting that person.

2. **Would Middle Eastern governments be barred from monitoring the communications of this Pakistani green-card holder by any U.S. law if he were inside one of those Middle Eastern countries? In other words, under the Wyden amendment, would it be the case that the law would permit every government in the world – other than our own – to monitor the communications of this Pakistani Al Qaeda member when he is in the Middle East?**

Answer: I am not aware of any United States law that would prohibit a foreign government from monitoring the communications of a U.S. lawful permanent resident who is an Al Qaeda member located in that country in the Middle East.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00092 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.033

3A. Again, considering the hypothetical example of a Pakistani national who resides in Pakistan but has acquired a green card: under the Wyden amendment, the United States would be required to get court pre-approval and a warrant if it wanted to monitor this Pakistani in Pakistan in the course of a foreign intelligence investigation. Now suppose that the U.S. thought that this Pakistani green card holder were participating in drug smuggling in Pakistan and the FBI opened a criminal investigation. Would the U.S. be required to obtain a warrant in order to monitor his activities in Pakistan in the course of a drug-smuggling criminal investigation?

Answer: No, courts have not imposed a requirement to obtain a warrant for surveillance conducted outside the United States for purposes of a criminal investigation.

Senator Wyden's amendment would require prior court approval to conduct certain foreign intelligence surveillance of U.S. persons overseas. Historically, this type of surveillance is conducted in accordance with executive orders that have been in place since before the enactment of FISA in 1978. Under those executive orders, Attorney General approval is required before foreign intelligence surveillance and searches may be conducted against a U.S. person abroad under circumstances in which a warrant would be required if conducted for law enforcement purposes. More specifically, section 2.5 of Executive Order 12333 requires that the Attorney General find probable cause that the U.S. person target is a foreign power or an agent of a foreign power. Such activity now generally falls under the requirements of section 704, described above.

B. What if this Pakistani national were believed to be involved in bribery of a public official while residing in Pakistan and the U.S. opened a criminal investigation of his activities. Would the U.S. be required to obtain a warrant to monitor such activities in Pakistan?

Answer: No. As I explained in the answer to 3(a) above, the United States is not required to obtain a warrant from a United States court to conduct surveillance outside the United States for purposes of a criminal investigation.

C. What if the U.S. thought that this green card holder were fencing stolen goods in Pakistan? Would the U.S. be required to obtain a warrant in order to monitor his activities in Pakistan?

Answer: No. As I explained in the answer to 3(a) above, the United States is not required to obtain a warrant from a United States court to conduct surveillance outside the United States for purposes of a criminal investigation.

4. As I understand it, the Wyden amendment would apply not just when Pakistan-to-Afghanistan communications are routed through the U.S. Rather, it would apply whenever the activities of a U.S. green card holder are monitored overseas as part of a terrorism investigation. As a result, even if the U.S. were participating with the

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00093 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.034

Pakistani government in an investigation inside Pakistan that targeted a Pakistani national who was a U.S. green-card holder, the U.S. would be required to report the investigation to the FISA court and seek a warrant.

I also understand that while many Middle Eastern governments cooperate with the United States in the war with Al Qaeda, many of these governments do not want other countries or radicalized elements of their own populations to know that they are helping the United Stats. As a result, many of these governments require that the fact of their cooperation with the United States or the details of joint counterterrorism operations not be disclosed outside of the U.S. intelligence community.

A. Would the Wyden amendment's requirement that the existence of intelligence investigations conducted entirely inside a foreign country be disclosed in U.S. court proceedings violate any of our information-sharing agreements with foreign intelligence services?

Answer: While a full answer to this question would require additional details regarding specific countries and could involve classified information, we would, of course, work closely with foreign governments to mitigate any potential effects of having to obtain court orders before conducting foreign intelligence surveillance abroad.

B. Should we expect that foreign intelligence services will refuse to share information or otherwise cooperate with the United States in the future if the Wyden amendment requires U.S. intelligence agencies to disseminate intelligence information outside of the intelligence community?

Answer: Please see the answer to question 4(A) above.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00094 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.035

SUBMISSIONS FOR THE RECORD

ASSOCIATION OF
RESEARCH LIBRARIES

Statement for the Record

to the U.S. Senate Committee on the Judiciary

for the hearing:

"FISA [Foreign Intelligence Surveillance Act] Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability."

Submitted by
the American Library Association and the Association of Research Libraries.

The American Library Association (ALA) and the Association of Research Libraries (ARL) (hereafter known as "the Libraries") submit this statement for the record to the Senate Judiciary Committee hearing titled "FISA [Foreign Intelligence Surveillance Act] Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability" on October 31, 2007.

Founded in 1876, the ALA is the oldest and largest library association in the world with 65,000 individual members and 4,000 library and corporate members dedicated to improving library services and promoting the public interest in a free and open information society.

The ARL is a nonprofit organization of 123 research libraries in North America. ARL's members include university libraries, public libraries, government and national libraries. ARL influences the changing environment of scholarly communication and the public policies that affect research libraries and the diverse communities they serve.

The Libraries seek language in FISA modernization proposals that ensures judicial review of law enforcement requests for library patron records or surveillance of library users through library networks. The Libraries strongly believe that when the government seeks foreign intelligence information from libraries in the United States, it should do so only on an order authorized by the Foreign Intelligence Surveillance Court (FISC), regardless of whether the person using the library services is a U.S. citizen or not, or located within the United States or abroad. Libraries are gateways to freedom abroad. They offer expanded services globally, provide distance learning opportunities, and serve American and foreign student communities abroad as part of their essential mission. And they rely on a global network of communications facilities and services to do so, but this should not make libraries into communications service providers as proposed under the FISA modernization efforts today.

52426.036

Existing State Privacy & Confidentiality Laws Yield to FISA
Libraries have deep and longstanding principles of protecting patron privacy. Privacy is essential to the exercise of free speech, free thought, and free association. In a library (physical or virtual), the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Forty-eight states and the District of Columbia have patron confidentiality laws; the attorneys general in the remaining two states have issued opinions recognizing the privacy of library users' records. Ten state constitutions guarantee a right of privacy or bar unreasonable intrusions into patrons' privacy. The courts have established a First Amendment right to receive information in a publicly funded library. Further, the courts have upheld the right to privacy based on the Bill of Rights of the U.S. Constitution.

Since the USA PATRIOT Act superseded these state laws, libraries have consistently argued for judicial supervision during the various debates on NSLs, CALEA, and the USA PATRIOT Act. Often the debate focuses on whether or not libraries are communications service providers. Libraries are not like commercial telephone and communications companies; they have a special place in our families' lives and in our Nation's history as providing special space to learn, explore, and inquire.

The Justice Department Treats Libraries as Communications Providers
The Department of Justice has consistently taken the position when libraries provide free public access to the Internet or email accounts to their users that they are "communications service providers." Libraries do not seek to thwart national security efforts nor to be safe havens for those engaging in illegal activities. However, because the mission of libraries is so closely bound to our Nation's first amendment freedoms, there should be judicial review of law enforcement demands for library records or communications. Libraries' services to users inevitably will rely on communications services, but this is incidental to providing library services as a whole just as the communications capability in Microsoft's XBox Live or Nintendo's Wii are incidental to the game play and does not render these game companies "communications service providers."

Past efforts to protect libraries from federal demands for information without court supervision failed because explicit statutory language was not included. For example, there are explicit statements in the USA PATRIOT Act Reauthorization debates detailing that libraries do "not fall under the purview of the NSL provision." Despite this clear Congressional intent, the FBI still contends that libraries remain subject to that Act's NSL provisions because the language of the statute was not explicit. Thus, legislation must expressly state that the term "communications service provider" does not include libraries, or it is unlikely to be respected by the Department of Justice.

FISA Modernization Should Clarify that Libraries are NOT Communications Providers
To the extent a library in the U.S. provides remote communications or access to communications services to U.S. or non-U.S. users abroad, under the FISA Amendments Act, like the PAA before it, such communications could be subject to warrantless seizure or interception from facilities in our libraries. Our position is simple – the government should not enter a library in the U.S. or access facilities used by libraries to conduct electronic surveillance on any library user,

regardless of where the user happens to be when using library services, without an order from the FISA court.

Libraries provide distance learning opportunities from facilities abroad to American and foreign student and faculty who access library services remotely in support of their educational and research activities. The library community is concerned that these opportunities and the chance to bring access to knowledge and freedom of expression abroad will be diminished if the U.S. government may, without a FISA court order or judicial oversight, monitor the use of library facilities by non-U.S. citizens abroad if the government believes the communication or usage concerns foreign intelligence.

This is not a hypothetical concern. U.S. universities have numerous educational programs throughout the world, and it is possible, if not likely, that student and faculty library users at those foreign campuses of U.S. institutions will be relying on servers or routers that reside in the stateside facilities. At the same time, the issue is not likely to arise so often that obtaining FISA court approval would impose reasonable burdens on or create obstructions to terrorism or foreign intelligence investigations.

Now as always in our history, reading and inquiry are among our greatest freedoms. Libraries, inherent to a democratic society, provide a place to exercise intellectual freedom: the free and open exchange of knowledge and information where individuals may exercise freedom of inquiry and the right to privacy and confidentiality with regards to information sought. A 2005 report released by ALA documents the ***chilling effect*** of law enforcement activity in libraries. "Impact and Analysis of Law Enforcement Activity in Academic and Public Libraries" found that library patrons are intimidated by intrusive measures such as the USA PATRIOT Act and National Security Letters (NSLs). This chilling effect can take many forms; for instance, a patron's concern about privacy of their library records may result in reluctance to checkout or view certain materials.

Any surveillance can have a chilling effect, but warrantless surveillance is particularly insidious. Libraries recognize that surveillance is a necessary tool today, but Congress must recognize that the requirement for a court order to enter a library at least would send a message of fairness and due process the world over.

Proposed Language

The following language is proposed as a means to resolve our concern, the addition of a single caveat to Section 105B: **"For purposes of this section, the term "communications provider" does not include a library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1))."**

American Library Association – Lynne Bradley, 202-628-8410
Association of Research Libraries – Prue Adler, 202-296-2296

Hearing of the

United States Senate
Committee on the Judiciary

FULL COMMITTEE HEARING

"FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability"

Wednesday, October 31, 2007

Testimony of Edward J. Black
President and CEO
Computer & Communications Industry Association

52426.039

Good morning, Mr. Chairman and Members of the Committee. My name is Ed Black. I have served as President and CEO of the Computer and Communications Industry Association for the past 12 years. CCIA is a nonprofit membership organization for a wide range of companies in the computer, Internet, information technology, and telecommunications industries. Since its founding in 1972, CCIA has consistently promoted innovation and competition through open markets, open systems, open networks. We appreciate this opportunity to help find the best balance of national security law and privacy rights.

The Internet is an unprecedented and unique force for democratic change and socio-economic progress. Increasingly, our nation's digital economy depends on the dynamism and openness of the Internet. That functionality is jeopardized if surveillance activities result in the chilling of free speech. In our society, all information services companies play a custodial role in promoting First Amendment rights. Internet functionality is further jeopardized if end users lose confidence in the security of their business and personal transactions online. The Fourth Amendment is key to preserving that privacy and network security. While constitutional considerations should be paramount, I will also emphasize some very practical business aspects of this debate over amendments to FISA.

We understand our industry's technology and the many wonderful ways in which can be used… and ways it can be misused. In addition to the most obvious domestic benefits, it

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00099 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.040

can be a tool for spreading freedom and democracy around the world, and from a foreign relations standpoint, the U.S. government needs to lead by example in promoting the freedom of ideas and communications that the Internet makes possible. However, that leadership will fall flat if we easily excuse unlawful surveillance in our own country. We urge you to consider that this legislation could weaken the hand of American companies that must contend with escalating demands for censorship and surveillance by foreign secret police.

CCIA supports current legislative efforts to amend FISA to achieve a sound balance between effective terrorist surveillance for our national security and Fourth Amendment privacy rights of Americans, while enhancing opportunities for the exercise of First Amendment freedoms. We should all want protection both from terrorists and from illegal spying, search and seizure by our own government. In crafting our efforts to combat terrorism, we should not forfeit our privacy or weaken our First or Fourth Amendment rights. As a nation, we should not countenance the sort of autocratic surveillance of ordinary citizens which we find so abhorrent in repressive foreign regimes. American electronic communications and information services companies understandably want protection from overreaching government demands to participate in illegal wiretapping or data mining. We want to be good citizens, but not police agents. But we need protection not just from third party liability for acquiescing to proper demands, but protection from improper government pressure or inducement as well. Industry needs clear constitutional ground rules that are subject to waiver only through transparent procedures and process.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00100 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.041

It might be useful to examine and compare how government agencies and the private sector deal with user/customer communications data and content. Of necessity for the provision of public services, government collects certain basic information on taxpayers, citizens, and businesses and other organizations that cannot be legally withheld by the individual or organization. Government agencies, recognizing the importance of privacy, observe many security procedures to protect personal privacy, but too often we have seen serious breaches in this security. Indeed, data mining, hacking, and inadvertent dissemination of information on U.S. citizens creates increasing security challenges for government at all levels. For the government, use of the information, not its confidentiality is paramount.

Internet commerce and the digital economy, on the other hand, fundamentally depend on maintaining the privacy and security of customers' personal information and business data. Private sector companies have information on customers that those customers expect will be kept private, unless they give consent, or a court order of some kind compels release of that personal information to law enforcement. Citizens seem willing to provide vast amounts of data to private institutions believing that these institutions act as a buffer between them and the government. Customers must be free to conduct their personal lives and business transactions without fear of illegal or widespread surveillance and spying. The high-tech industry wants to help our government protect Americans from terrorists. However, companies cannot provide such assistance if network security is compromised because the rules for wiretapping and surveillance are expendable at the

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00101 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.042

discretion of the President, or subject to ongoing controversy and flux. In a sense, the economic and social consequences of a reduction in network security would be a partial victory for the very terrorists we are seeking to defeat.

To be sure, the Director of National Intelligence (DNI) requires the assistance of private communications companies. But those companies must be free to insist on constitutionally solid procedures that are clear and transparent, so they are not reduced to guesswork about the applicability of immunity under the FISA statute. Clear lines of separation and differentiation between public sector and private sector roles in surveillance activities are therefore essential to a robust Internet and a free society.

Private companies, be they in health care, financial services, hard goods retailing, or information services should not become arms of the federal government, regularly turning over customer information, or "sitting on" phone lines. The many companies which are part of our Internet and communications systems must be trusted carriers and repositories of Americans' free speech. Commercial telecommunications and Internet services are not fair territory for direct involvement by the federal government. Put another way, outsourcing to private companies the collection of Americans' call records and communications messages for government use is both unconstitutional and destructive to valuable, and indeed essential, network security.

The role of private sector institutions as a vigilant buffer between excessive government demands and the rights of our customers is a role to be protected, not undermined.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00102 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.043

In the interest of national security there is broad agreement on our government's right to conduct surveillance of foreign targets, especially terrorists, and to collect and share such information even when obtained without court approval. FISA was created for the express purpose of limiting executive privilege regarding surveillance of U.S. citizens. The FISA Court and the Attorney General provide checks and balances in this separation of powers. Since 9/11 2001, the Bush Administration has had many years to work with Congress on important revisions to the FISA law. That opportunity was squandered, however, in favor of a unilateral secret National Security Administration (NSA) spying program. When high-level internal debate ensued over the legality of that program, it was covered up. Even the private sector companies who were being asked to assist may not have been aware of the controversy.

CCIA believes that HR 3773, the RESTORE Act of 2007, which is now under consideration in the House of Representatives, offers careful and enlightened updating of FISA. The Senate Intelligence Committee legislation, S. 2248, while providing some important improvements over the hastily passed Protect America Act (PAA) of last August, allows surveillance based on executive certification, without a court order. And, disturbingly, the bill provides retroactive immunity from civil liability for those who may have participated in an illegal program, without identifying what conduct is being immunized.

The Executive Branch has the primary burden to establish that requests for data are on strong legal footing, under the Fourth Amendment and FISA, and do not amount to

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00103 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.044

illegal search and seizure of U.S. citizens private information. But the Bush Administration apparently did not present independent judicial legal authorization to some of the companies involved. The Administration simply "certified" the program was legal. And some very large companies with legions of their own lawyers either did not double check, or, well, we just don't know what transpired. Apparently Qwest did run a legal reality check, and concluded some of the executive requests were out of line. Whatever letters were used to request assistance have not been shared with the House Judiciary Committee or any Member of the House of Representatives to date. Senate Intelligence Committee members only merited a limited look at these documents immediately prior to their vote on S. 2248. We understand that the leadership of the Senate Judiciary Committee, after a year of ignored or rejected formal requests, finally was offered a look at some of the relevant documents late last week. But none of us know about what type of debates, if any, took place between the government and the companies involved, or within the companies.

We think there are important lessons that can be learned from what has transpired over the last several years. Learning these lessons will help us draw the lines of proper conduct for the future. Alternatively, if we make up the rules as we go along, ANY violation of the constitution performed to serve a compelling national security or law enforcement purpose can be rationalized and covered up by retroactive immunity. Under this scenario, private industry effectively becomes the judge, weighing whether particular purposes are sufficiently compelling to risk unconstitutional searches. The government doesn't want that; neither do we.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00104 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.045

Retroactive immunity for participation in the recent secret government surveillance program is premature at best, since this Congress has yet to become well-informed enough to determine whether in fact the NSA surveillance program exceeded legal boundaries established under FISA. If immunity for past activities is granted prior to full disclosure and accountability from the Executive Branch, Congress and the public may never understand the nature of the NSA warrantless wiretapping program.

We also believe broad retroactive immunity would be ill advised in any event because it would perpetuate uncertainty, confusion and second-guessing in the future. Commercial enterprises and individual employees have the right to insist on clear judicial authorization before complying with requests for information or communications otherwise protected by customer privacy guarantees. And companies would know that in getting judicial authorization, they will avoid having to petition for additional extra-statutory immunity later. But if retroactive immunity is granted in this case, future extralegal emergency requests will be accompanied by a wink and a promise of similar immunity after things settle down.

Understandably, some companies want this immunity badly. Their motives may have been as honorable as their legal analysis was lax, but we don't know enough at this point to make a judgment. We do know, however, that some of the companies involved, when they want something from the government, be it immunity from liability or further deregulation, tend to threaten a parade of horribles that will arise if they are not granted

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00105 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.046

the desired relief. When the prize is sweeping deregulation, we hear that without it, they will have no more incentive to invest in broadband network infrastructure. When the goal is immunity from participation in the NSA program, they threaten that without it, they will be reluctant to co-operate in the future. But as long as electronic communications companies are presented with clear legal authorization in the future, they should have every reason to provide the network assistance that is so important to our national security. Hence, Congress must establish bright, constitutional lines identifying industry's responsibility.

With regard to claims of possible bankruptcy, it makes sense for Congress to at least consider a statutory cap on damages that might be awarded to plaintiffs for information wrongly provided in a past NSA program, especially following a finding of good faith by a federal judge. In any future consideration of immunity from liability for participation in government surveillance, small businesses and individuals should have a lighter burden of establishing they acted in good faith in a response to a high-level government request.

The civil litigation should be allowed to proceed. Even if major portions of the proceedings need to be held in camera and the scope of discovery narrowed, judges - and to the extent compatible with serious national security concerns, the public - should learn what really happened in these cases.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00106 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.047

Conclusion

Millions of workers in our industry believe that we are an industry that can be strong positive force for our society. The underlying desire to facilitate communications, the transfer of information and knowledge, and the building of bridges across cultural boundaries: these are core motivations of people in our industry. These motivations are part of why our industry is successful. The economic rewards can be great but they are as much a consequence as they are a motive.

To sustain this positive force, we must work together to establish processes and protections for private personal and business information that is so critical to the open and free use of the Internet. To disclose private information, our industry needs clear and constitutionally proper ground rules that are only deviated from through well-defined transparent processes. These rules must be straightforward enough to be publicized and understood by U.S. citizens and businesspeople who may be called upon to assist their government in these uncertain times.

NOTE: The views expressed herein do not necessarily represent the position of every individual CCIA member company.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00107 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.048

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
PRINCIPAL DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE
(ACTING)
WASHINGTON, DC 20511

SEP 2 7 2007

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

Dear Mr. Chairman:

Thank you for your letter of September 24, 2007 to the Director of National Intelligence (DNI) regarding the discussion at your Committee's hearing on the Protect America Act and an incident in which proceeding under the Foreign Intelligence Surveillance Act (FISA) to collect on foreign targets abroad delayed the initiation of coverage expected to reveal the communications of Iraqi insurgents who had kidnapped U.S. soldiers. By providing this event as an example, the DNI hoped to provide some context as to why the authorities provided by the Protect America Act are critical to protect the nation.

In particular, in the hearing before the House Judiciary Committee on September 18, 2007, the DNI provided the following example: "American soldiers [were] captured in Iraq by insurgents, and we found ourselves in a position where we had to get a warrant to target the communications of the insurgents." The DNI explained that the process of obtaining a court order put the Intelligence Community (IC) in a difficult position.

In the hearing before your Committee on September 20, 2007, the DNI was asked to discuss this example further. In that testimony, the DNI explained that this example demonstrated that FISA has put us in a position where "[w]e are extending Fourth Amendment rights to a terrorist foreigner, foreign country, who's captured U.S. soldiers, and we're now going through a process to produce probable cause...." The Director further explained the greater context, which is that FISA, because it has not kept pace with technology, requires that the IC meet a probable cause standard in situations where no substantial privacy right of an American is at issue. Moreover, the DNI endeavored to explain that while useful, the emergency provisions of FISA still require a finding of probable cause that the target of the collection is an agent of a foreign power.

The timeline you have proposed releasing publicly contains a number of additional details that the DNI did not discuss in open session. If you believe that the public release of this timeline will help to further inform the debate, the IC does not object. Indeed, Director McConnell tried to be as open as possible in his testimonies because we understand that these issues are of utmost importance to the Congress and to the public. In the interest of protecting sensitive sources and methods, however, we have made some minor modifications to your original proposal, which are attached.

Some aspects of the proposed timeline also deserve clarification. The timeline that you provided may give the impression that the process of obtaining the emergency authorization

52426.049

under FISA began at 10:00 a.m. on May 15, 2007. In fact, the process began earlier, as evidenced by the source material provided to the Committee by the National Security Agency on June 8, 2007. On May 14, 2007, as soon as specific leads had been identified, analysts began to compile all the necessary information to establish the factual basis for issuance of a FISA court order as required by the emergency authorization provision of the statute.

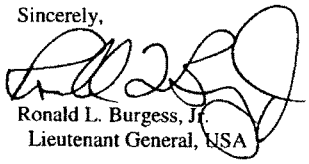
As the Committee is aware, the circumstances of this case presented novel and complicated issues. These issues, which needed to be evaluated before the emergency authorization could be requested, distinguished this situation from a typical case of targeting non-U.S. persons abroad. This was the focus of the internal Executive Branch deliberations between 12:53 p.m. and 5:15 p.m. and the reason behind the decision to contact the Attorney General for emergency authority rather than the Solicitor General.

While admittedly this was a complex situation, the Director used this example to illustrate the point that, due to changes in technology, the FISA statute extends privacy protections to foreign terrorists located outside the United States merely because FISA makes a geographic distinction based on the location of the collection. Novel issues aside – in order to comply with the law – the Government was required to spend valuable time obtaining an emergency authorization as required by FISA to engage in collection related to the kidnapping.

The Committee has received extensive, in-depth briefings and detailed documentation concerning this case over the past months. The professionals, both in the IC and at the Department of Justice, analyzed the facts and legal issues presented in this situation as they are required to do under the law. FISA's emergency provision, while extremely useful, still requires a determination before the Attorney General can authorize the collection that there is a factual and legal basis for granting FISA authority. Failure to ensure that the facts and the legal issues of this case satisfied FISA's requirements could have exposed these professionals to criminal penalties.[1]

We appreciate the time and effort you have spent on this important issue and we look forward to working with you further to make the authorities provided by the Protect America Act permanent. If you have any questions on this matter, please contact the Director of Legislative Affairs, Kathleen Turner, who can be reached on (202) 201-1698.

Sincerely,



Ronald L. Burgess, Jr.
Lieutenant General, USA

Enclosure

cc: The Honorable Peter Hoekstra

[1] See 50 U.S.C. § 1809 (providing criminal sanctions for intentionally engaging in electronic surveillance under color of law except as authorized by statute).

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00109 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.050

- On May 12. 2007, after a coordinated attack on their position south of Baghdad, three U.S. soldiers were reported missing and believed to have been captured by Iraqi insurgents. Immediately upon learning of the attack, theater-based and national SIGINT assets responded by dedicating all available resources to obtaining intelligence concerning the attack.

- On May 13 and 14, 2007, the Intelligence Community began to develop additional leads concerning the communications of insurgents claiming responsibility for the attack, including approaching the FISA Court on May 14 for an amendment to a then-current order with some bearing on the hostage situation. The amendment was granted that day.

- As soon as specific leads had been identified, analysts began to compile all the necessary information to establish the factual basis for issuance of a FISA court order as required by the emergency authorization provision of the statute.

- On May 15, 2007:

    - At 10:00 a.m., key U.S. agencies met to discuss and develop various options for collecting additional intelligence relating to the kidnapping by accessing certain communications.

    - At 10:52 a.m., the NSA notified the Department of Justice (DOJ) of its desire to collect some communications that require a FISA order.

    - It was determined that some FISA coverage already existed.

    - At 12:53 p.m., the NSA General Counsel agreed that all of the requirements for an emergency FISA authorization had been met for the remaining collection of the communications inside the U.S.

    - From 12:53 p.m. to 5:15 p.m. Administration lawyers and intelligence officials discussed various legal and operational issues associated with the surveillance.

    - At 5:15 p.m, the DOJ's FISA office – the Office of Intelligence Policy and Review (OIPR) – received a call formally requesting emergency authority to conduct surveillance.

    - At 5:30 p.m., the OIPR attorney on duty attempted to reach the Solicitor General who was the Acting Attorney General while Attorney General Gonzales was addressing a United States Attorney's Conference in Texas. However, the Solicitor General had left for the day and the decision was made to attempt to reach Attorney General Gonzales in Texas.

    - The OIPR attorney then contacted the Justice Department Command

52426.051

Center and requested that the Command Center locate the Attorney General in Texas. After several telephone calls with the staff accompanying the Attorney General, the OIPR lawyers were able to speak directly with the Attorney General and brief him on the facts of the emergency request.

- At 7:18 p.m., the Attorney General authorized the requested surveillance. The Justice Department attorneys immediately notified the FBI.

- At 7:28p.m, the FBI notified key intelligence agencies and personnel of the approval.

- At 7:38 p.m., surveillance began.

52426.052

Senator Christopher J. Dodd
Testimony before the Senate Judiciary Committee
The FISA Amendments Act of 2007

Mr. Chairman, Ranking Member Specter, and distinguished members of the Judiciary Committee:

Thank you for this opportunity to share with the Committee my deep misgivings over S. 2248, the FISA Amendments Act of 2007. Today's hearing is extremely important as the Senate once again considers amending the Foreign Intelligence Surveillance Act.

I believe the FISA Amendments Act of 2007, as currently written, embodies an egregious break with the rule of law: It grants retroactive immunity to telecommunications companies who cooperated with the Administration's warrantless wiretapping policy -- turning over the private records of a large number of their customers to U.S. authorities.

The retroactive immunity provision is especially troubling for three reasons. First, it sets the dangerous precedent of placing a few large corporations above the law. In my view, Congress should not intervene in the ongoing civil disputes about the role of these companies in the President's Terrorist Surveillance Program. It is important that the Congress allow the courts to determine whether or not some of our fellow citizens' rights were violated by the actions of the telecommunications companies. There is simply no compelling reason for the legislative branch to short-circuit the workings of the courts.

52426.053

Second, passing this legislation effectively endorses the president's insupportable reading of the Constitution. The president appears to believe that he has the authority to disregard valid, constitutional laws if they at cross purposes with what he asserts are his executive powers. As we have seen time and time again, this view has undermined the rule of law. I believe that if the Congress grants retroactive immunity, we will undermine the principle that we are a nation of laws not men. If companies were complicit with the President in disregarding the law, they should not be immunized from the legal consequences of their actions.

Third, and perhaps most astoundingly, Congress is being asked to excuse the actions of the telecommunications companies before we even know exactly what those actions were. The president is asking us to endorse his continuing effort to keep Americans in the dark. As Louis Fisher, a specialist in Constitutional Law with the Law Library of the Library of Congress recently explained to the *Washington Post*, "It's particularly unusual in the case of the telecoms because you don't really know what you're immunizing. You don't know what you're cleaning up." We should not eliminate the right of our fellow citizens to have their day in court, nor should we grant immunity when we do not have a full understanding of the implications of doing so. At the very least, before any vote, every Senator should have the opportunity to review the documents that the Administration is using to justify the warrantless wiretapping program.

For all of these reasons, retroactive immunity must be stripped from this bill. In addition, there are several other provisions that deserve to be scrutinized by the Judiciary

52426.054

Committee. Most notably, the provisions of this bill do not expire until 2013, meaning that an entire presidential term will have passed before we'll again have the opportunity to change this misguided policy.

While the current legislation is an improvement over the Protect America Act, more work remains to be done. Congress is once again being offered a false choice—liberty for security. As the Committee continues to work on this legislation, I respectively request that the retroactive immunity provisions be removed.

Thank you, Chairman Leahy and Ranking Member Specter, for the opportunity to express my heartfelt views before your distinguished committee.

52426.055

CHRISTOPHER J. DODD
CONNECTICUT

COMMITTEES:
BANKING, HOUSING, AND URBAN AFFAIRS
FOREIGN RELATIONS
HEALTH, EDUCATION, LABOR, AND PENSIONS
RULES AND ADMINISTRATION

United States Senate
WASHINGTON, DC 20510-0702

WASHINGTON OFFICE:
448 RUSSELL SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-2823
TDD (202) 224-5964

STATE OFFICE:
30 LEWIS STREET, SUITE 101
HARTFORD, CT 06103
(860) 258-6940
TDD (860) 528-7459

HOME PAGE: http://dodd.senate.gov
E-MAIL: http://dodd.senate.gov/webform

October 30, 2007

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate

Dear Chairman Leahy,

I am writing to you today requesting that you include my enclosed statement regarding S. 2248, the FISA Amendments Act of 2007, as part of the record at the Judiciary Committee's hearing on Wednesday, October 31, 2007.

As you know, I have expressed my strong opposition to the provisions in the bill reported by the Select Committee on Intelligence granting retroactive immunity for telecommunications companies. It is my hope that the Judiciary Committee, under your leadership, will remove these provisions from the bill.

I look forward to working with you and other members of the Judiciary Committee as the Senate considers this important legislation. Again, thank you for your consideration of my request.

Sincerely,

Chris

CHRISTOPHER J. DODD
UNITED STATES SENATOR

PRINTED ON RECYCLED PAPER

52426.056

October 29, 2007

The Honorable Patrick J. Leahy
Chairman, Committee on the Judiciary
The Honorable Arlen Specter
Ranking Member, Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Chairman Leahy and Ranking Member Specter:

We are writing to support the carrier immunity provision passed with bipartisan support in the FISA reform legislation recently reported out by the Senate Select Committee on Intelligence (SSCI) and now before your Committee for consideration. We believe that the carrier immunity provision not only provides a just and fair protection for companies that allegedly responded to a call for assistance from the President in a time of national crisis, but also is a necessary policy for promoting the national security interests of the United States.

Telecommunications carriers who allegedly participated in what has become known publicly as the "Terrorist Surveillance Program" have been sued in over forty lawsuits seeking hundreds of billions of dollars in damages. Beyond the existence of an intelligence program involving electronic surveillance, which the President has confirmed, we cannot, of course, confirm anything further in this letter, including whether or not any telecommunications carriers even participated in such a program. The fact remains, however, that carriers are facing years of expensive litigation and potentially ruinous damages based upon allegations of their involvement in an intelligence program authorized by the President, reviewed for legality at the highest levels of the Executive Branch, and represented to the carriers to be lawful. We believe these lawsuits should not be allowed to proceed.

Protecting carriers who allegedly responded to the government's call for assistance in the wake of the devastating attacks of September 11, 2001 and during the continuing threat of further attacks is simply the right thing to do. When corporations are asked to assist the intelligence community based on a program authorized by the President himself and based on assurances that the program has been determined to be lawful at the highest levels of the Executive Branch, they should be able to rely on those representations and accept the determinations of the Government as to the legality of their actions. The common law has long recognized immunity for private citizens who respond to a call for assistance from a public officer in the course of his duty. The salutary purpose of such a rule is to recognize that private persons should be encouraged to offer assistance to a public officer in a crisis and should not be held accountable if it later turns out that the public officer made a mistake. That principle surely applies here, especially given the limited nature of the immunity contemplated in the bill, which would apply only where carriers were told that a program was authorized by the President and determined to be lawful.

Failing to provide immunity to the carriers will produce perverse incentives that risk damage to our national security. If carriers now named in lawsuits are not protected for any

52426.057

The Honorable Patrick J. Leahy
The Honorable Arlen Specter
October 29, 2007
Page 2

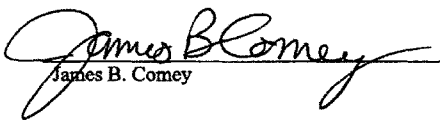
actions they allegedly may have taken in good faith reliance on representations from the Government, both telecommunications carriers and other corporations in the future will think twice before assisting any agency of the intelligence community seeking information. In the fight against terrorism, information private companies have -- particularly in the telecommunications field -- is a vital resource to the Nation. If immunity is not provided, it is likely that, in the future, the private sector will not provide assistance swiftly and willingly, and critical time in obtaining information will be lost. We wholeheartedly agree with the assessment of the report accompanying the bill from SSCI: "The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation." S. Rep. 110-209, at 11.

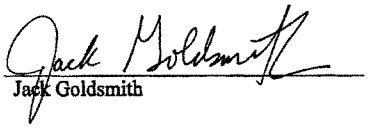
Finally, we note that we are familiar with the legal analysis conducted within the Executive Branch of intelligence activities allegedly connected to the lawsuits against telecommunications carriers and with debates within the Executive Branch about that analysis. Given our experiences, we can certainly understand that reasonable people may question and wish to probe the legal bases for such intelligence activities. We firmly believe, however, that the best place for that examination and debate is not in a public lawsuit against private companies that were asked to assist their Nation, but within the Executive branch, where intelligence-gathering decisions are made, and in joint efforts between the Executive Branch and Congress to ensure appropriate oversight.

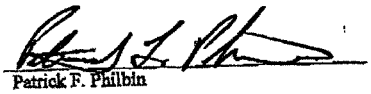
For all of these reasons, we encourage the Committee to approve the carrier immunity provision as a fair, just, and equitable result that properly promotes a policy of encouraging the private sector to cooperate with the intelligence community.

Sincerely,

John D. Ashcroft


James B. Comey


Jack Goldsmith


Patrick F. Philbin

52426.058

Statement
United States Senate Committee on the Judiciary
FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability
October 31, 2007

The Honorable Russ Feingold
United States Senator , Wisconsin

Contact: Zach Lowe (202) 224-8657

Statement of U.S. Senator Russell D. Feingold
Senate Judiciary Committee Hearing on
"FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability"

October 31, 2007

As Submitted for the Record

Mr. Chairman, I am very pleased that the Judiciary Committee is holding this public hearing on the critically important issue of amending the Foreign Intelligence Surveillance Act (FISA). We considered possible amendments to FISA at a hearing in September where we discussed them with Director McConnell, but now that specific legislation has been reported from the Senate Select Committee on Intelligence, I applaud you for taking the opportunity to evaluate it carefully in this Committee.

I sit on the Intelligence Committee, and I agree that some of its work must be conducted behind closed doors due to the sensitive nature of the information that committee handles on a regular basis. But the Intelligence Committee should have considered the FISA legislation in a more open process. The Committee would have benefited from the input not just of the Administration, but also of outside experts who may have brought a different point of view to consideration of the legislation.

So I am particularly glad that the Judiciary Committee is holding this open hearing, and that its upcoming markup will also be in an open setting. The public should have the ability to see what we are doing on this very important issue. In addition, this committee's expertise in privacy and civil liberties, and FISA, is crucial to this debate.

This committee's consideration is also important because the bill reported by the Intelligence Committee, which I voted against, is badly flawed. Senator Wyden and I summarized our opposition in our "Minority Views" on the bill:

We support the underlying purpose of FISA reform: to permit the government to conduct surveillance of foreign targets, particularly terrorist suspects, as they communicate with other persons overseas, without having to obtain a FISA court order. We believe that this purpose can be achieved while protecting the rights and privacy of law-abiding Americans conducting international communications. We believe that the bill that passed the Senate Intelligence Committee unfortunately falls short of that goal in some respects, and we are also concerned that it also provides sweeping retroactive immunity to those alleged to have cooperated with the President's warrantless wiretapping program. We were therefore disappointed with the bill and voted against it.

It is my hope that the Judiciary Committee will pass a better bill. Congress should never have passed the so-called Protect America Act, even for six months. We should fix this law to make sure we protect Americans' privacy as we wiretap terrorists and other foreign intelligence targets. We also should not be granting unjustified retroactive immunity for those alleged to have cooperated with the Administration's illegal warrantless wiretapping program. Let's get it right this time.

Thank you, Mr. Chairman.

Testimony of Morton H. Halperin

Before

The Senate Committee on the Judiciary

October 31, 2007

Mr. Chairman,

It is a great pleasure for me to appear once again before this distinguished committee to discuss the latest effort to modify FISA so that it continues to protect both our security and our liberty. This committee has found a way to protect both in the past and I am confident that it can do so again with the cooperation of those concerned about civil liberties and those charged with defending our security.

To assist in that effort, I want to propose a way of thinking about the structure of FISA and review the history of how the two major sets of issues raised by FISA have been treated.

The two major questions are: (1) What electronic communications should the government be able to acquire using procedures different from those mandated for criminal investigations; and (2) what procedures should be put in place so that all concerned groups can know clearly what the rules are and have confidence that the rules are being followed? In making some suggestions for what should be in the legislation I will focus on the second set of questions.

Pre-FISA Procedures

It is important to begin by recalling the pre-FISA world and to understand the pressures which led two administrations, large bi-partisan groups in both Houses of the Congress, and many civil libertarians to support the enactment of FISA.

In the period before FISA was enacted in 1978 there were essentially no legislated rules and only the most rudimentary procedures in the Executive branch establishing standards for when communications could be acquired. We now know that the FBI conducted surveillance of targets such as the Soviet Ambassador, Martin Luther King, Jr., steel company executives, journalists and government officials, including, I should add in the spirit of full disclosure, me when I worked in the Nixon Administration and then as a private citizen. The National Security Agency also acquired copies of telegrams entering and leaving the United States relating to anti-war activists.

52426.060

The Justice Department did have formal procedures for the Attorney General to approve a warrantless surveillance, but often more informal procedures would be used—perhaps a decision by the Director of the FBI on his own or a request from a White House official to the Director.

Government communication with the telephone company – at the time, AT&T was the only one -- could not have been more casual. A designated official of the FBI called a designated official of AT&T and passed on a phone number. Within minutes all of the calls from that number were being routed to the local FBI field office and monitored. The fruits of the surveillance were routed to the officials who requested the surveillance.

The viability of this system came to an end with the Watergate scandals and the resulting revelations of the improper actions of the intelligence community. At the time, there were many leaks or reports of improper surveillance. Government officials were not certain about which surveillance activities were legal and what behavior might subject them to civil or criminal penalties. Many lawsuits were being filed and the legality of the surveillances were being challenged in criminal cases. The phone company was being sued and was beginning to demand clarity as to what its obligations were.

(All this should sound very familiar)

Enactment of FISA

The Ford Administration came to the conclusion that it was time to subject this set of activities to the rule of law. Intelligence professionals objected: they were reluctant to submit to formal rules and especially to the requirement that they get prior judicial approval before they could act, unless there was an emergency. They feared that the resulting rules might prevent them from acting as necessary. Civil libertarians were concerned that the rules might authorize surveillance that went beyond the Fourth Amendment or was open to abuse. They feared the court would be a rubber stamp and that the oversight would not be sufficient.

In the end, after multi-hearings in this and other committees, Congress was able to craft a bill that has stood the test of time. The legislation answered both questions – who could be surveilled and with what safeguards – with great clarity and in a way that struck, in my view, the right balance.

It provided that communications of foreign powers or agents of a foreign power could be acquired in the United States for the purpose of collecting foreign intelligence information. No surveillance was permitted of those without connections to foreign powers, including people suspected of leaking information. The basic procedure required approval by the Attorney General

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00120 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.061

and then approval of the FISA court, with periodic re-approvals and supervision by the Court to determine that the rules were being followed. There were also standards for a few limited situations when a surveillance could be started or conducted without a court order. These were carefully delimitated and involved emergencies, leased lines, and the Congress declaring war.

AT&T received the clarity that it sought and deserved. The rule, spelled out clearly in several places in the legislation and well understood by all, was this: If AT&T received a copy of a warrant or a certification under the statute, it was required to cooperate. If it did not receive authorization by means outlined in the statute, it was to refuse to cooperate and was to be subjected to state and federal civil and criminal penalties for unlawful acquisition of electronic communications.

Let me say a further word about the certification option since it seems to be a source of some misunderstanding and therefore needs, I will suggest, to be clarified in the current legislation.

Everyone involved in the drafting understood that there was a need to provide great clarity and simplicity to the phone company. The simplest rule would have mandated that the phone company act only with a warrant. However, there clearly were situations where speed or exigency did not permit time for a warrant and a few cases where it was agreed that a warrant should not be necessary. For those cases, the statute provided that the telephone company should cooperate if it received a certification from the Attorney General. However, it was clear from the legislation (or should have been) that the Attorney General could provide a certification only if the specific requirements of FISA had been met and he needed to assure the company that those statutory requirements had been met.

Experience under FISA

From the time that FISA went into effect until President Bush authorized a warrantless surveillance program which violated its rules, FISA was extraordinarily successful. There was not a single leak of a FISA program or surveillance. According to the testimony of successive government officials, many more communications were intercepted and used by the intelligence community under FISA than had been the case before its enactment. There were no suggestions of abuse and government officials and private companies participated in the program with no doubts and no fear of incurring penalties. There were few, if any, civil suits, and in criminal cases the courts almost uniformly upheld the statute.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00121 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.082

Operating Outside of FISA

All that changed to the detriment of both our liberty and our security when the Administration decided to act outside of FISA rather than seeking amendments to the statute. Since the authorization of the warrantless surveillance program, there have been leaks to the press and lawsuits filed. Government officials have doubted whether the programs they have been asked to implement were legal. Private companies are under siege and in doubt about their legal obligations. Programs have been terminated or altered because they were viewed as illegal by government officials or the FISA court. Senior White House officials even visited an ailing Attorney General in his hospital room to ask him in vain to authorize a warrantless surveillance program.

Restoring FISA

To protect our security and our liberty we must restore the FISA process. It is a welcome sign of progress that the Administration asked for new legislation and seems to be ready to conduct all of its surveillance pursuant to the new law enacted by the Congress. However, the administration continues to attack those with a different view as unpatriotic or political and fails to explain why the language it proposes is necessary or even what it means. This is true of the Act passed in haste in August and, I regret to say, it is true of some of the language of the bill reported by the Senate Special Committee on Intelligence (SSCI).

This committee has the opportunity, which I urge you to seize, to return to the traditions of FISA and to report out a bill that restores the trust of the American people and protects both our security and our liberty by providing clear rules.

As I said at the outset, FISA legislation involves two major questions. First, under what circumstances may the government acquire electronic surveillance and second, what are the rules for how it can acquire those communications.

On the first question, the major change proposed by the administration and reflected in both the SSCI and House bills is to permit the acquisition from a wire in the United States of communications by targeting a person overseas without a particularized court order based on probable cause even if this involves intercepting conversations and communications of persons in the United States. There is an on-going debate about whether this change is necessary and constitutional. I propose to leave that discussion to others and to focus my remaining remarks on the procedures and rules for monitoring compliance, assuming that the committee will authorize the new surveillance program.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00122 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.063

The SSCI bill, in my view, falls short of providing the clarity and the effective oversight that is necessary to protect our security and our liberty and to secure the trust of the American people. Let me focus on four major concerns:

1. The statement in Section 701 that "Nothing in the definition of electronic surveillance under section 101 (f) shall be construed to encompass surveillance that is targeted in accordance with this title at a person reasonably believed to be located outside the United States."

2. The failure to require that a court order must be obtained in advance of any surveillance under this new authority (except in emergencies), to provide that service providers must receive the court order before they can cooperate, and to permit effective court oversight of the surveillance process.

3. The failure to provide for effective procedures and oversight to insure that the government may not use this procedure when it is in fact seeking to acquire the communications of a U.S. person or a person in the United States.

4. The failure to eliminate the ambiguity in the statute so as to make it clear that the procedures in FISA are the sole means to conduct electronic surveillance for intelligence purposes and that private companies must cooperate if they receive a court order or a certification specifically authorized by this statute and must not cooperate in any other circumstance.

Section 701

With all due respect to the drafters of Section 701 of the proposed legislation (who continue to be anonymous), it can only be described as Alice in Wonderland. It says that the language in FISA, which defines "electronic surveillance," means not what it clearly says, but what the current bill says that it says. Later, in two places the reported bill says that electronic surveillance has the meaning from FISA and that the change in the definition should be ignored Moreover, no reason to write the bill this way is presented in the Committee Report or elsewhere that I am aware of, or by the administration. The intended purpose can be accomplished by much more explicit language as I will discuss.

The FISA definition of electronic surveillance includes the following:

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00123 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.064

Section 701 of the bill reported by SSCI reads as follows:

"Limitation on the Definition of Electronic Surveillance."
"Nothing in the definition of electronic surveillance under section 101 (f) shall be construed to encompass surveillance that is targeted in accordance with this title at a person reasonably believed to be located outside the United States."

In other words, even though the plain language of 101 (f) (2) covers all acquisitions from wire in the United States if either person is in the United States, the language in the reported bill asserts that it does not cover such an interception if it is directed at a person outside the United States. This is clearly a change in the definition and not a "limitation" on the definition as the SSCI bill labels it or a "clarification" of the definition as the Protect America Act (PAA) headed it.

Having said that words do not mean what they clearly do mean, the bill in two other sections says, "never mind." That is, as the Committee Report puts it, the bill "negates that limitation for the matters covered by those sections" that deal with the use of the information in criminal trials and exclusivity. However, there is no such "negation" of the "limitation" for the sections of FISA that establish criminal and civil penalties. Thus, the only result of this convoluted language might be to negate the possibility of civil or criminal penalties for illegal acquisition of this information. There is no reason to believe that this was the Committee's intent.

Language in a bill that says the legislation should not be "construed" in a certain way is useful if the language of the legislation is ambiguous or if there is a fear that the Executive branch or the courts might construe the language to imply something that was not intended. For example, in retrospect it would have been useful for Congress to have said in the Authorization to Use Military Force (AUMF) that it should not be" construed" as amending FISA. However, when the intent is to change the law it should be done in a straightforward way so there can be no ambiguity as to what was intended. This is especially important when we are dealing with civil liberties.

This result can be achieved simply by striking Section 701 and changing Section 703 (g) (2) (A) (vi) -- which sets out the requirements for the certification to be given to the FISA court – to read, " the surveillance is targeted at persons reasonably believed to be located outside the United States."

I urge the committee to ask the administration how their understanding of what the statute required would change if the legislation was amended in this way.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00124 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.065

The Role of the FISA Court

The SSCI bill has important provisions which begin to re-establish an appropriate role for the FISA court, but much more needs to be done if the court is to be able to play its essential role in providing assurance to service providers and to the public that the rules established by the Congress are being followed.

The government should be required to go the FISA court first and to get approval from the court before it begins surveillance, except in an emergency situation. By definition, if there is no emergency, there is time to go to the court and there is no reason to allow the executive branch to begin a surveillance without first having court approval. Requiring as a matter of routine that court approval must come first will assure that the executive branch gives the matter the full consideration that it deserves before starting a surveillance which will lead to the acquisition of many conversations and communications of persons in the United States and Americans abroad. Moreover, requiring the executive to go to the court before beginning a surveillance would enable Congress to require that the service providers cooperate only if they have a court order or a certification in an emergency.

I cannot imagine any public policy argument to the contrary once one concedes that the court needs to play a role and there is an exception for emergencies with ample time limits. The SSCI Committee Report does not provide any rationale and I have not seen any from the Administration except the general statement that they do not want to be burdened. That is clearly not a sufficient reason in a constitutional democracy.

One consequence of the failure of the bill to require prior judicial authorization is that it also fails to empower the court to cut off surveillance that is illegal under the statute. Under proposed Section 703(j)(5)(B) the government can repeatedly submit new guidelines to the court every 30 days, and the court cannot order the surveillance to stop because the government can elect to continue it while it adjusts its procedures repeatedly.

Second, the legislation needs to make clear that the FISA court has continuing supervisory authority to insure that the surveillance is being conducted consistent with the statute. The court's authority to seek additional information and to order changes in the surveillance activity should not be left in doubt. The court should be able to supervise the minimization procedures and whatever procedures there are to insure that the communications of persons in the United States and Americans anywhere are not inappropriately acquired.

Let me turn to that issue.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00125 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.086

Communications of Persons in the United States

If Congress extends beyond the period of the PAA the authority to acquire wire communications in the United States without individual warrants, it must take additional steps to insure that the communications of persons in the United States are not inappropriately acquired or disseminated beyond the NSA collection process.

There are, I think, two major concerns. One is abuse. There is legitimate concern that this vast power will be used to acquire communications of innocent Americans and used for political purposes. I see no suggestion that this has been done since 9/11, but the history of past abuses suggests that Congress needs to keep this concern in mind as it grants substantial additional powers to the Executive branch.

The second concern is how to deal with the conversations of U.S. persons and persons in the United States. At one end of the spectrum is an interception that is truly incidental and is not disseminated in a way that reveals the identity of the American. At the other end of the spectrum would be the intentional targeting of a person known to be in the United States. The bill does very little to deal with the vast space in between.

It is not easy to come up with an effective standard for when a regular FISA warrant should be required. That is the strongest reason, in my view, to have a much shorter sunset time for this new grant of authority. Congress must be in a position in a short time to assess how this balance is working and to determine if additional safeguards are needed.

There are several additional steps that I urge the committee to take to deal with this serious concern.

First, I urge you to adopt the provision included in the House bill which requires that guidelines be adopted and approved by the FISA court that "will be used to ensure that an application is filed under section 104, if otherwise required by this Act, when a significant purpose of an acquisition is to acquire the communications of a specific person reasonably believed to be located in the United States."

In other words, if the intelligence community wants to acquire the communications of a specific person in the United States, it must get a standard FISA warrant based on probable cause that one of the communicants is a foreign power or the agent of a foreign power. This seems to be a reasonable operational definition of when the acquisition of communications is no longer incidental. I am not aware of any specific response from the intelligence community to this language and urge the committee to seek an evaluation of its impact on the proposed program.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00126 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.067

Second, the committee should provide for record keeping which will enable the court, the committees and others to more effectively monitor this process. This should include requiring that records be kept of all "unmasking" of the identities of U.S. persons from communications acquired by this program. Records should also be kept and reported regularly of the number of persons in the U.S. whose communications are disseminated as well as the number of times in which the target of the communication actually turned out to be in the United States or to be a U.S. person abroad.

I urge the Committee to consider two additional steps. First, you should consider creating a presumption, to be monitored by the FISA court, that if the NSA disseminates more than three conversations of the same U.S. person, that person has become a subject of interest to the intelligence community so that a warrant would be required to disseminate additional conversations or to intentionally acquire them. I suggest a presumption because I think the government should be able to show that for some particular reason the dissemination is appropriate.

Finally, I urge you to consider a limitation on the types of foreign intelligence information that can be disseminated from this program if it concerns a U.S. person. Since the need for this new authority arose as a result of the new demands following 9/11, there is every reason to consider limiting the new authority to collecting information related to international terrorism. If that is not done, at the very least there should be a limit on the kinds of information about Americans derived from their conversations that can be disseminated.

The appropriate divide is between information in (e) (1) as opposed to (2) of the FISA definition of foreign intelligence information. FISA established this breakdown precisely to distinguish between information about activities that were inherently illegal, such as espionage, sabotage or terrorism, as compared to the information in (2) which deals with information of interest to the intelligence community about national security or foreign policy but which includes many innocent conversations among, for example, experts on a particular country.

Exclusive Means

Let me turn finally to the question of exclusive means. Here I want to associate myself with the very thoughtful additional views of Senators Feinstein, Snowe and Hagel to the SSCI Report.

I believe, as they do, that the original FISA legislation was as clear as legislation can be. Congress intended that the means that it provided would be the exclusive means for conducting electronic surveillance for intelligence purposes. When it referred to "other statutes" it meant the criminal laws, and

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00127 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.088

when it referred to "certifications that a warrant was not required and that the statutory requirements had been met" it meant the statutory requirements of FISA and not of another statute.

Nonetheless, because both the Executive branch and, apparently, the service providers claim to have read FISA differently, Congress should take some additional steps beyond those in the SSCI bill to make clear to all concerned that Congress intends the means authorized by FISA to be the sole means to conduct this surveillance.

It is particularly important to do this if the Congress is going to grant some form of relief to the service providers for their past behavior. Indeed I think it is essential that the service providers publicly and unequivocally acknowledge that in the future they will be liable for civil and criminal penalties if they cooperate with the intelligence community outside the procedures of FISA.

Here are the additional steps that I suggest:

1. As I have already proposed, eliminate Sec. 701. This is essential to avoid any suggestion that electronic communication conducted for intelligence purposes in the United States is not covered by the exclusivity provisions or by the criminal and civil penalties.

2. At each place in FISA where Congress grants authority to conduct electronic surveillance without a court order, add a phase specifying that the certification given to a service provider must specify the specific statutory provisions being relied on and that the specific requirements of that section have been met. This will prevent the Attorney General from providing a general certification that the surveillance is lawful.

3. Add general language that the requirements of FISA can be amended only by legislation enacted after the enactment of these amendments that specifically refers to FISA and specifically amends the authority to conduct electronic surveillance. This would make impossible the kind of specious argument made by the government that the AUMF somehow amended FISA and make it unnecessary to say in every bill passed later that it should not be construed so as to authorize surveillance outside of the FISA procedures.

4. Amend the section of FISA that provides for criminal and civil penalties for cooperation outside of the FISA procedures. Here is the proposed change to 2511 (2) (a) (ii) (B) dealing with cooperation permitted without a court order:

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by [law] a specific provision of the Foreign Intelligence Surveillance Act

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00128 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.089

, specifying the provision and stating that all statutory requirements of that specific provision have been met, and that the specified assistance is required.

This change would eliminate any possible intentional or unintentional misreading of the clear intent of the language. Service provides and government officials alike would be on notice that they can cooperate with a surveillance only if there is a court order or the government is acting pursuant to the specific requirements of a provision of FISA which authorizes surveillance without a court order, either temporarily while a warrant is obtained or under circumstances, such as the lease line exception, where the statute does not require a court order, and that the requirements of that provision have been satisfied.

Taken together and with what is already in the SSCI bill, I believe the language would provide the strongest possible assertion of exclusive means while sending a totally unambiguous message to service providers that in the future they should not come to Congress for relief if they cooperate outside the requirements of this legislation.

Conclusion

Mr. Chairman, I appreciate very much this opportunity to testify before this Committee and present views on possible amendments to FISA. At the same time I am aware that there are many other individuals and groups with a deep interest in FISA whose views are not necessarily identical to those presented in my statement. I trust the committee will consider those views as well, as it debates this critical legislation.

I would, of course, be delighted to respond to your questions or to submit any additional information for the record.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00129 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.070

STATEMENT OF CHAIRMAN PATRICK LEAHY,
SENATE JUDICIARY COMMITTEE,
HEARING ON
"FISA AMENDMENTS: HOW TO PROTECT AMERICANS' SECURITY AND PRIVACY AND PRESERVE THE RULE OF LAW AND GOVERNMENT ACCOUNTABILITY"
OCTOBER 31, 2007

The Foreign Intelligence Surveillance Act – FISA – is intended to protect both our national security and the privacy and civil liberties of Americans.

Changes to that law must be considered carefully and openly – not eviscerated in secret Administration interpretations or compromised through fear or intimidation. The so-called Protect America Act, passed just before the summer recess, was an example of the worst way to consider changes to FISA. It was hurriedly passed under intense, partisan pressure from the Administration. It provides sweeping new powers to the government to engage in surveillance – without warrants – of international calls to and from the United States involving Americans, and it provided no meaningful protection for the privacy and civil liberties of the Americans who are on those calls.

Fortunately, the Protect America Act will expire early next year. This is the Committee's second hearing to inform our consideration of possible legislation to take the place of that flawed Act. Of course we must accommodate legitimate national security concerns and the need for flexibility in surveillance of overseas targets, but Congress should do that in a way that protects the civil liberties of Americans.

I commend the House Committees and the Senate Select Committees on Intelligence for seeking to incorporate the better ideas from our work this summer into their current legislative proposals. The House of Representatives is considering the "RESTORE Act," which appears to take a fair and balanced approach -- allowing flexibility for the Intelligence Community while providing oversight and protection for Americans' privacy. The Senate Select Committee on Intelligence has also reported a bill that makes improvements to the current temporary law. Increasing the role of the FISA Court and oversight by the Inspector General and the Congress are matters we should have incorporated this summer.

At the outset I should acknowledge the grave concern I have with one aspect of S.2248. It seeks to grant immunity – or, as Senator Dodd has called it, "amnesty" -- for telecommunications carriers for their warrantless surveillance activities from 2001 through this summer, which would seem to be contrary to FISA and in violation of the privacy rights of Americans.

Before even considering such a proposal, Senator Specter and I have always been clear with the Administration that we would need the legal justifications, authorizations, and other documents that show the basis for the actions of the government and the carriers. Since the existence of the President's secret wiretapping program became public in

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00130 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.071

December 2005, this Committee has sought that relevant information through oral and written requests and by conducting oversight hearings. After our repeated requests did not yield the information the Committee requested, we authorized and issued subpoenas for documents related to the legal justification for the President's program.

Finally, this week, the Administration has belatedly responded. Senators on the Committee and designated staff have begun to receive access to legal opinions and documents concerning authorization and reauthorization of the program. This is a significant step, though long overdue.

I am considering carefully what we are learning from these materials. The Congress should be careful not to provide an incentive for future unlawful corporate activity by giving the impression that if corporations violate the law and disregard the rights of Americans, they will be given an after-the-fact free pass. If Americans' privacy is to mean anything, and if the rule of law is to be respected, that would be the wrong result.

A retroactive grant of immunity or preemption of state regulators does more than let the carriers off the hook. Immunity is designed to shield this Administration from any accountability for conducting surveillance outside the law. It could make it impossible for Americans whose privacy has been violated illegally to seek meaningful redress.

The lawsuits that would be dismissed as a result of such a grant of immunity are perhaps the only avenue that exists for an outside review of the government's program and honest assessment of its legal arguments. That kind of assessment is critical if our government is to be held accountable. One of my chief inquiries before deciding to support any legislation on this subject is whether it will foster government accountability. Anyone who proposes letting the telecommunications carriers off the hook or preempting state authorities has a responsibility to propose a manner to test the legality of the government's program and to determine whether it did harm to the rights of Americans.

Safeguarding the new powers we are giving to our government is far more than just an academic exercise. The FISA law itself is testament to the fact that unchecked government power leads to abuse. The FISA was enacted in the wake of earlier scandals, when the rights and privacy of Americans were trampled while no one was watching. We in the Senate, and on this Committee, have a solemn responsibility to hundreds of millions of our fellow citizens. Because the American people's rights, freedom and privacy are easily lost; but once lost, they are difficult to win back.

I look forward to the testimony of our witnesses and thank them for appearing.

# # # # #

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00131 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.072

Hearing Before the United States Senate Committee on the Judiciary

Re: "FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability."

October 31, 2007

Prepared Statement of Patrick F. Philbin, former Associate Deputy Attorney General, U.S. Department of Justice.

Chairman Leahy, Ranking Member Specter, and Members of the Committee, I appreciate the opportunity to address the matters before the Committee today. I gained experience with issues related to the Foreign Intelligence Surveillance Act and the importance of electronic surveillance as an intelligence tool during my service at the Department of Justice from 2001 to 2005. My duties both as a Deputy Assistant Attorney General in the Office of Legal Counsel and, subsequently, as an Associate Deputy Attorney General involved providing advice on issues related to FISA and the use of electronic surveillance in intelligence and counterterrorism activities. Since my return to the private sector, I have continued to pay close attention to developments in this area, such as recent judicial decisions imposing heightened burdens on the U.S. government with regard to the monitoring of communications from foreign sources, and the filing of multiple lawsuits seeking to hold private telecommunications carriers liable for providing assistance to the government in its surveillance activities.

Electronic surveillance is an important tool both for preventing terrorist attacks and for rooting out espionage. At the same time, it is an intrusive technique that, if not properly constrained and controlled, can threaten the privacy and liberties of American citizens. Ensuring that electronic surveillance remains an agile and adaptable tool for the intelligence community in a world of ever-evolving technology while at the same time protecting American liberties is the challenge that Congress faces in amending FISA.

52426.073

In my testimony, I wish to make three main points:

First, I want to express support for the provisions in the Bill that will allow the Executive to target the communications of persons reasonably believed to be overseas without first going to the FISA court. These provisions are consistent with FISA's original purpose and are necessary to ensure that FISA does not fall out of step with changing technology. They provide a medium-term solution to the problems that motivated Congress's enactment of a short-term fix in the Protect America Act earlier this year.

Second, I want to express my support for the provisions in Senate Bill 2248 that would grant immunity to telecommunications carriers against lawsuits based on the carriers' alleged participation in the "Terrorist Surveillance Program" authorized by the President. In essence, those lawsuits seek to hold carriers liable to the tune of billions of dollars for their patriotic decision to cooperate with U.S. government operations that Executive Branch officials had determined to be lawful and necessary. Whether or not those determinations by Executive Branch officials were correct in every instance is not a matter that should be addressed through private lawsuits against the carriers. To the contrary, allowing such lawsuits to proceed would be fundamentally unfair to carriers who are alleged to have cooperated in reliance on representations from the Executive Branch that their activities were lawful. Worse, it would provide a perverse incentive that would threaten to deter future cooperation with the government in times of emergency.

Third, however, I also want to note one provision of the bill that I consider unwise -- the provision that would create a wholly new requirement for the government to obtain an order from the FISA court before monitoring communications of U.S. citizens who are overseas. When government officials have sufficient basis to believe that U.S. citizens overseas are

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00133 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.074

engaging in espionage or terrorist activities, they should be able to act expeditiously in conducting necessary surveillance, and should not be required to go before the FISA court. Historically, such surveillance powers have been exercised for limited purposes and, as far as I am aware, there has been no suggestion of any abuse warranting this change in the law. Accordingly, I believe there is no need to expand the FISA Court's jurisdiction and to constrain the capabilities of the Executive in this way.

I. S. 2248 Appropriately Provides That No Individualized Order Need Be Sought for Surveillance of Foreign Targets Reasonably Believed To Be Outside the United States

One of the central features in the pending legislation lies in provisions that allow the Attorney General and the Director of National Intelligence to authorize the targeting for surveillance purposes of foreign terrorists and other foreign intelligence targets reasonably believed to be located outside the United States, without obtaining individualized court orders from the Foreign Intelligence Surveillance Court. The Protect America Act was a short-term fix to address this same issue. In my view, given changes in technology, a longer-term solution to make the application of FISA less dependent on the medium used to carry a communication (such as wire vs. radio waves), and more directly tied to the location of the target, is definitely warranted, and this provision is a good start.

The pending legislation provides a medium-term solution to this problem. Among other relevant provisions, Section 701 generally removes from the definition of "electronic surveillance," to which FISA's procedures would otherwise apply, surveillance activities targeted at a person "reasonably believed to be located outside the United States." Accordingly, for the majority of surveillance activities targeted at persons outside the United States, there would be no requirement to obtain an individualized court order.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00134 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.075

This is consistent with the original intent of FISA that warrants not be required for interception of foreign communications. In 1978, when Congress enacted FISA, foreign communications and even international communications were usually collected and monitored through interception of radio and microwave transmissions, for which no warrant was necessary. Now, those same communications are often routed through fiber-optic cables that regularly pass through the United States. This technological change should not make a difference to the legal constraints our laws place on collection. Just as it was in 1978, the underlying principle now should be that where the government is targeting foreign terrorists and foreign intelligence targets, it should be able to proceed more expeditiously than when it targets persons within our country's borders. The Bill as drafted is generally consistent with this principle and makes a needed change for the efficient use of electronic surveillance as an intelligence tool.

II. S. 2248's Provision of Immunity for Telecommunications Carriers Is Fair and Critically Promotes the National Security Interests of the United States

I also support the provisions in S. 2248 providing immunity for telecommunications carriers who allegedly participated in what has become known publicly as the "Terrorist Surveillance Program" and for other alleged intelligence activities involving electronic surveillance. These carriers have been sued in over forty lawsuits seeking hundreds of billions of dollars in damages. The pending actions are currently consolidated in the Northern District of California in *In re National Security Agency Telecommunications Records Litigation*, MDL No. 06-1791. Of course, the extent to which carriers actually did or did not participate in such a "Terrorist Surveillance Program" remains classified. The fact remains, however, that the carriers are facing years of expensive litigation and claims for potentially ruinous damages based upon allegations that they did nothing more than furnish assistance requested by the government,

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00135 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.076

authorized by the President, reviewed for legality at the highest levels of the Executive Branch, and represented to the carriers to be lawful.

Title II of the pending legislation would address this problem by allowing the Attorney General to step in and obtain the dismissal of these lawsuits. Under Section 202, a civil action challenging a telecommunication carrier's assistance in a government intelligence activity must be dismissed if the Attorney General certifies to the pertinent court either that the carrier did not provide the alleged assistance, or that the allegations of the lawsuit concern an intelligence activity (i) authorized by the President between September 11, 2001 and January 17, 2007, (ii) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States, and (iii) described in a written request to the carrier from the Attorney General or a high-ranking intelligence official indicating that the intelligence activity was authorized by the President and had been determined to be lawful. There are several reasons why it is sound policy to retain this provision in the pending legislation.

First, protecting carriers who allegedly responded to the government's call for assistance in the wake of the devastating attacks of September 11, 2001 and during the continuing threat of further attacks is simply the right thing to do. Determining the single right thing to do has always been my touchstone for decision making, and I believe it provides the correct answer here. The allegations here are that, in the wake of the devastating attacks of 9/11, corporations were asked to assist the intelligence community based on a program authorized by the President himself and based on assurances that the program had been determined to be lawful at the highest levels of the Executive Branch. Under those circumstances, the corporations should be entitled to rely on those representations and accept the determinations of the Government as to the legality of their actions. They should not be penalized for responding patriotically in a time

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00136 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.077

of crisis and relying on the Government's own assessment of the legality of their actions. Having obtained assurance from the Government that their conduct is lawful, they should not be forced to defend themselves against protracted litigation by persons whose primary grievance lies with the Government.

Granting immunity to the telecommunications carriers here is consistent with the immunity that the common law has long recognized for private citizens who respond to a call for assistance from a public officer in the course of his duty. The salutary purpose of such a rule is to recognize that private persons should be encouraged to offer assistance to a public officer in a crisis and should not be held accountable if it later turns out that the public officer made a mistake. The rule ensures, in the words of Justice Cardozo, that "the citizenry may be called upon to enforce the justice of the State, not faintly and with lagging steps, but honestly and bravely and with whatever implements and facilities are convenient and at hand." *Babbington v. Yellow Taxi Corp.*, 250 N.Y. 14, 17 (1928).

Smith v. Nixon, 606 F.2d 1183 (D.C. Cir. 1979), is illustrative of the way courts have dealt with such matters. In that case the United States Court of Appeals for the District of Columbia Circuit upheld the dismissal of a telephone company from a case that challenged the wiretapping of a home telephone. While suggesting that the wiretap itself might have been illegal, the Court of Appeals held that the company still could not be held liable because it "did not initiate the surveillance, and it was assured by the highest Executive officials in this nation that the action was legal." *Id.* at 1191. Similar principles surely apply here, especially given the limited nature of the immunity contemplated in the bill, which would apply only where carriers were told that a program was authorized by the President and determined to be lawful.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00137 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.078

In light of existing precedent regarding qualified immunity, some might argue that there is no need for Congress to enact a specific provision providing immunity to telecommunications carriers here. But this argument overlooks the point that even litigating questions of qualified immunity can prove burdensome; and there is also a real possibility that courts would misapply qualified immunity doctrines and rule against the carriers. Even if the telecommunications carriers ultimately prevail, moreover, the specter of protracted litigation over such questions could serve to deter future cooperation with government officials in times of emergency. The pending legislation thus wisely provides for dismissal after the filing of a duly executed government certification.

Second, immunity is appropriate because allowing the suits to proceed would risk leaking sensitive national security information. As the suits progress, they will inevitably risk disclosure of intelligence sources and methods that will damage the national security of the United States in the midst of its ongoing struggle with al Qaeda. The assertion of state secrets privilege is not a cure-all for protecting national security information, as some decisions in the suits have already shown. The longer the suits proceed, the more details concerning the ways the intelligence community may seek information from the Nation's telecommunications infrastructure will leak. Our enemies are far from stupid; as such information trickles out, they will adapt their communications security to thwart our surveillance measures, and valuable intelligence will be lost.

Third, failing to provide immunity to the carriers here would also discourage both communications companies and other private sector corporations from providing assistance in the context of future emergencies, thus damaging the national security of the United States and potentially putting American lives at risk. In the continuing struggle with Al Qaeda, one of our

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00138 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.079

Nation's greatest strategic assets is its private sector and the information that sector has available to it. Particularly in this war with a shadowy enemy, intelligence is vital for success. If immunity is not provided, however, it is likely that, in the future, private sector corporations will prove much more reluctant to provide assistance swiftly and willingly, and critical time in obtaining information will be lost. I agree fully with the conclusion in the report accompanying the bill from the Select Committee on Intelligence: "The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation." S. Rep. 110-209, at 11.

Finally, I disagree with the suggestions made by some that the private lawsuits against carriers can force the carriers to serve a gatekeeper role to second-guess and provide, in essence, oversight on the intelligence-gathering decisions of the Executive. I believe that approach is misguided. As a general matter, telecommunications carriers are simply not well-positioned to second-guess government decisions regarding the propriety or legality of intelligence activities. I know from experience that the legal questions involved in such matters are highly specialized, extremely difficult, often involve difficult constitutional questions of separation of powers and are not readily susceptible for analysis by lawyers at a company whose primary concern is providing communications service to the public. We should not adopt policies that give private corporations incentives to demand detailed information from the Executive and in essence to conduct their own mini-investigations into the propriety of intelligence operations the government wishes to conduct. As explained above, such incentives would be at cross-purposes with the government's need for expedition.

At the same time, there must be some mechanism for addressing concerns raised about the program at issue. Some have raised questions about the underlying legitimacy of the

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00139 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.080

surveillance program in which various telecommunications carriers allegedly participated, and about the legal reasoning of the government officials involved in establishing and overseeing that program. As the Committee is likely aware, I am intimately familiar with the legal analysis conducted within the Executive Branch of the intelligence program in question and with debates about that analysis, both within the Executive Branch and in Congress. I can understand that what has leaked about the program might lead reasonable people to want further probing into the legal bases for the program. And ensuring that all intelligence activities do strictly adhere to the law is an imperative. But the question of liability for telecommunications carriers is logically and legally entirely distinct from that debate and should be decided wholly apart from it. The mechanism for addressing legal concerns about the intelligence programs is through rigorous oversight within the Executive Branch -- which, I might add, does actually work -- and through a joint effort between the Executive and Congress to ensure appropriate oversight. The Executive and Congress are the branches constitutionally charged with responsibility in these fields, and they should appropriately address questions about intelligence activities, not leave those matters vital for national security to be sorted out in private lawsuits.

The mechanism that is least suited for addressing concerns about the Executive Branch's legal decisions, and least likely to produce outcomes that rationally address the national security imperatives of the Nation, is private lawsuits conducted in public forums seeking to obtain money damages from private entities who were not responsible for the intelligence-gathering decisions made by the Executive Branch.

III. S. Bill 2248 Should Be Amended To Remove the Requirement That a Warrant Be Obtained To Conduct Surveillance of U.S. Citizens Overseas

There is one respect, however, in which S. Bill 2248 departs from historical practice and from the underlying principles motivating the passage of FISA in 1978. Significantly,

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00140 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.081

subsection 703(c)(2) of the bill requires the government to obtain a warrant from the FISA Court in order to conduct surveillance of a U.S. citizen who is reasonably believed to be *outside the United States*. To obtain such a warrant the Attorney General must submit to the FISA Court an application setting forth facts demonstrating that there is probable cause that the target of the surveillance is an agent of a foreign power or terrorist organization. This is a new requirement, introduced in the Select Committee on Intelligence by way of an amendment to the original bill, and it would expand the FISA Court's jurisdiction in ways that have not before been tested.

In my view this requirement is inconsistent with our historical practice and unwarranted. As for history, under Executive Order 12333, which President Reagan signed in 1981, the Attorney General was permitted to authorize surveillance of U.S. citizens both within the United States and overseas upon a finding of probable cause to believe that the person in question is an agent of a foreign power. Such determinations have been handled outside of the FISA framework and without resort to the FISA Court. This system has worked well in allowing us to move flexibly and expeditiously to collect valuable intelligence on U.S. citizens who unfortunately choose to align themselves with foreign powers or terrorists. This system is consistent with the President's independent authority to conduct intelligence activities in the course of conducting United States foreign policy and acting to counter foreign threats. *See, e.g., In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surveillance Ct. of Review 2002) (describing the inherent authority of the President of the United States to gather foreign intelligence information).

At the same time, there has been no demonstration that the power to conduct limited surveillance of U.S. citizens overseas without resort to the FISA Court has led to abuse. Attorneys General have exercised their powers under Executive Order 12333 with judgment and

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00141 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.082

discretion. They have not targeted ordinary tourists or businesspeople engaged in routine overseas travel; instead, this authority has been used sparingly and appropriately. In light of the limited purposes for which surveillance of U.S. citizens overseas is conducted, coupled with the lack of evidence of abuse, there is no reason to impair the flexibility of highly sensitive intelligence and counterterrorism investigations by adopting a warrant requirement in this context. Nor is a warrant required by the Fourth Amendment. The touchstone of the Fourth Amendment is reasonableness. And it has long been held that in foreign intelligence investigations, the President may order warrantless searches consistent with the Fourth Amendment. That result can only apply more strongly to searches overseas. Accordingly, I recommend that the Senate amend the bill to remove this provision.

* * *

Thank you, Mr. Chairman, for the opportunity to address the Committee. I would be happy to address any questions the Committee may have.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00142 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.083

STATEMENT OF:
WILLIAM H. SORRELL, VERMONT ATTORNEY GENERAL;
G. STEVEN ROWE, MAINE ATTORNEY GENERAL;
RICHARD BLUMENTHAL, CONNECTICUT ATTORNEY GENERAL;
ANNE MILGRAM, NEW JERSEY ATTORNEY GENERAL;
ROBERT M. CLAYTON, III, COMMISSIONER, MISSOURI PUBLIC SERVICE COMMISSION

BEFORE THE

UNITED STATES SENATE
JUDICIARY COMMITTEE

FISA AMENDMENTS ACT OF 2007

Wednesday, October 31, 2007
Washington, D.C.

Chairman Leahy, Ranking Member Specter, and members of the Committee: Thank you for this opportunity to address you today on the proposed Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2007. In sum, we have grave concerns about the sweeping immunity from state investigations the Act would provide to electronic communications service providers (ECSPs) and others. We are particularly troubled by Section 204 of the Act (adding FISA § 803), which purports to preempt the well-established police powers of the states to regulate utilities doing business within their borders and safeguard the privacy and confidential information of their citizens. We urge you to remove Section 204 and preserve the appropriate balance of federal and state authority underlying our federalist system.

As the Committee is no doubt aware, we are presently representing our states in multidistrict litigation pending before the Honorable Vaughn R. Walker, Chief Judge of the Northern District of California, entitled *In re National Security Agency Telecommunications Records Litigation*, MDL Docket No. 06-1791 VRW.[1] The course of this litigation to date provides an object lesson on why the proposed preemption provision is inappropriate and unnecessary. Judge Walker's handling of the case demonstrates the wisdom of allowing the judiciary to continue to fulfill its role of policing the delicate balance between state and federal power and of weighing the competing policy concerns raised by the need for utilities regulation and consumer protection on the one hand and federal law enforcement and intelligence gathering on the other. To illustrate this point, we briefly summarize the litigation below.

Following citizen inquiries concerning possible unlawful disclosures of confidential telephone calling data, regulators in each state initiated administrative proceedings (and in Missouri a case was filed in state court) to determine whether local

[1] Similar proceedings commenced in Missouri and were also consolidated into the multidistrict litigation. Attorneys from the Missouri Public Service Commission are litigating those matters on behalf of Commissioner Clayton.

52426.084

telecommunications companies had violated state law. In response, the federal government filed actions in federal district court seeking declaratory and injunctive relief aimed at halting the state proceedings. Ultimately, these cases were consolidated for adjudication before Chief Judge Walker.

The government argued that federal law preempted the state proceedings because the states were invading areas of exclusive federal control and hindering the government's national security and intelligence gathering functions. In fact, the subjects of the investigations are utilities over which each state has plenary jurisdiction. Moreover, the purpose of each state investigation is to ascertain whether any carrier has violated state law by making unauthorized disclosures, without regard to the identity of the ultimate recipient of the disclosure. And the investigations do not seek details of any intelligence activity conducted by the federal government.

Judge Walker rejected the federal government's preemption arguments, holding that "Congress did not intend to foreclose state involvement in the area of surveillance regulation" and that "the investigations do not require an act by the carriers that federal law or policy deems unlawful. Nor do the investigations pose an obstacle to the purposes and objectives of Congress." *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 2007 WL 2127345, *12, *15 (N.D. Cal. July 24, 2007) (slip copy). The court recognized that the states' authority to regulate telecommunications companies' compliance with state law could not be foreclosed because a company might have assisted an intelligence-gathering operation. Indeed, to rule otherwise would eviscerate the states' longstanding police power over consumer protection (including privacy) and utilities regulation. *See New Orleans Pub. Serv., Inc. v. Council of City of New Orleans*, 491 U.S. 350, 365 (1989) ("[T]he regulation of utilities is one of the most important of the functions traditionally associated with the police power of the States."); *Florida Lime & Avocado Growers v. Paul*, 373 U.S. 132, 150 (1973).

In addition to preemption, the federal government argued that the state secrets privilege precluded the states' inquiries, although this privilege has never been formally asserted by the federal government in any of the state officials' cases. Judge Walker declined to rule on how the state secrets privilege would impact the state proceedings until the Ninth Circuit Court of Appeals renders its decision in an appeal from the court's decision in *Hepting v. AT&T*, 439 F. Supp. 2d 974 (N.D. Cal. 2006) (Walker, C.J.), concerning the applicability of the privilege in suits filed by individuals against telecommunications companies.[2] More specifically, the court observed that at least "some questions posed in these investigations fall outside the privilege's scope, a point the government conceded at oral argument," while noting that the states acknowledged that "some of the information sought . . . may implicate the state secrets privilege." *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 2007 WL 2127345 at *18. Accordingly, the court deferred on deciding "whether and to what extent the state investigations may proceed," *id.*, pending further guidance from the Ninth Circuit.

[2] The Ninth Circuit heard argument in *Hepting* on August 15, 2007.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00144 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.085

As the litigation illustrates, the court system, armed with protective doctrines like the state secrets privilege, is well-equipped to balance, on a case-by-case basis, society's interest in ferreting out and addressing illegal disclosures of confidential information with its interest in shielding legitimate, necessary disclosures and safeguarding state secrets.[3] Indeed, in assessing an assertion of the state secrets privilege, courts can conduct ex parte, in camera review of sensitive information. And a review of the pertinent caselaw reveals that the courts have successfully avoided information leaks in cases in which they considered state secrets privilege claims.

By contrast, proposed § 803 is an unnecessarily blunt instrument. To begin with, the proposed preemption provision (FISA § 803) wrongly assumes that it would be harmful to the public interest to disclose any information whatsoever relating to an ECSP's provision of assistance to an element of the intelligence community. Judge Walker rightly rejected this overreaching assertion. While the extent of appropriate disclosures (for example, the identity of affected individuals and details of the assistance rendered) may be subject to debate, there is no support for the complete preclusion of any disclosure whatsoever. Society benefits in numerous ways from the transparency promoted by the states' investigative powers. Those powers should not be limited without the most compelling justification, and none can be advanced on behalf of § 803.

Moreover, the operative language employed in proposed § 803 is vague and invites self-serving and unverifiable assertions by ECSPs. Specifically, subsections (1), (2), and (4) are triggered by investigations touching on an ECSP's "*alleged* assistance to an element of the intelligence community." (Emphasis added.) The nonspecific use of the adjective "alleged" to qualify the term "assistance" raises a question as to whether an entity under investigation could scuttle the inquiry at its discretion, merely by *alleging* that its response would call for disclosure of its "assistance." The provision required no showing by an ECSP or by the Attorney General. In short, the vagueness of the provision invites overbroad or unsubstantiated assertions and would almost certainly result in litigation over its meaning and scope.

Finally, no justification exists for providing less protections for state investigations than are provided to private plaintiffs under the proposed provisions of the Act. The proposed preemption provision appears to set a lower threshold for derailing the exercise of the states' traditional police powers than is required to invoke immunity against a private lawsuit. The immunity provisions (FISA §§ 703(h)(3), 802; FISA Amendments Act § 202) require the filing of a certification from the Attorney General or the Director of National Intelligence in the litigation and provide for judicial review of certifications. The states' interests in the exercise of their sovereign powers are certainly no less compelling than a private plaintiff's. In fact, they are arguably greater and grounded in fundamental principles of constitutional law. In addition, under current law the federal government can proceed in federal court if it concludes that a state

[3] For example, some of the initial information requests by the state regulators asked the carriers whether they had shared confidential information with the NSA. The court is now poised to assess whether and, if so, to what extent such requests violate the state secrets privilege. The court could also provide guidance on how such requests could be reformulated to pass muster.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00145 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.086

investigation implicates state secrets. Thus, the proposed preemption provision is not only antithetical to our constitutional allocation of state and federal power, but also unnecessary.

In sum, the courts are in the best position to strike an appropriate balance between the state and federal interests and have shown that they are sensitive to both. The proposed preemption provision should be deleted in its entirety.

Very truly yours,

William H. Sorrell Attorney General State of Vermont	Richard Blumenthal Attorney General State of Connecticut

G. Steven Rowe Attorney General State of Maine	Anne Milgram Attorney General State of New Jersey	Robert M. Clayton, III Commissioner Missouri Public Service Commission

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00146 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.087

Department of Justice

STATEMENT OF

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

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

PRESENTED

OCTOBER 31, 2007

52426.088

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

CONCERNING

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

BEFORE THE

COMMITTEE ON THE JUDICIARY

OCTOBER 31, 2007

Chairman Leahy, Ranking Member Specter, and Members of the Committee, thank you for this opportunity to testify concerning the modernization of the Foreign Intelligence Surveillance Act of 1978 (more commonly referred to as "FISA"). We appreciate the attention that Congress has given to this issue and the process that has led to the thoughtful bipartisan bill voted out of the Intelligence Committee on October 18, 2007, The FISA Amendments Act of 2007 (S. 2248).

Introduction

As you are aware, the Government's foreign intelligence surveillance activities are a vital part of its efforts to keep the nation safe from international terrorists and other threats to the national security. These surveillance activities provide critical information regarding the plans and identities of terrorists who conspire to kill Americans at home and abroad, and they allow us to glimpse inside terrorist organizations and obtain information about how those groups function and receive support—information that is key to tracking these organizations and disrupting their operations. In addition, our surveillance activities allow us to collect intelligence on the

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00148 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.089

intentions and capabilities of other foreign adversaries who pose a threat to the United States.

Prior to the passage of the Protect America Act of 2007 (PAA) in August, the difficulties we faced with FISA's outdated provisions—*i.e.*, the extension of FISA's requirements to surveillance targeting foreign intelligence targets overseas—substantially impeded the Intelligence Community's ability to collect effectively the foreign intelligence information necessary to protect the Nation. In April of this year, the Director of National Intelligence (DNI) submitted to Congress a comprehensive proposal to modernize the statute. The DNI, the Director of the National Security Agency (NSA), the general counsels of ODNI and NSA, and I testified before the Senate Select Committee on Intelligence regarding that proposal in May.

Recognizing the need to address this issue, Congress passed the Protect America Act, and the President signed the Act on August 5, 2007. The authorities you provided in the Protect America Act have allowed our intelligence agencies to collect vital foreign intelligence information, and the Act already has made the Nation safer by enabling the Intelligence Community to close gaps in our foreign intelligence collection. That Act, however, will expire in three months. To ensure that the Intelligence Community can obtain the information it needs to keep the Nation safe, the Administration strongly supports the reauthorization of the core authorities provided by the Protect America Act.

In addition, we urge Congress to enact the other important reforms to FISA contained in the proposal the Administration submitted to Congress in April; in particular, it is imperative that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11th attacks. By permanently modernizing and streamlining FISA, we can improve our efforts to gather intelligence on those who seek to harm us, and do so in a manner that protects the civil liberties of Americans.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00149 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.090

We value the opportunity to work closely with Congress on these important issues. Since the passage of the Protect America Act, Congress has held numerous hearings on the implications of that Act, the scope of the authorities granted by that Act, and other issues related to FISA modernization, and various officials from the Executive Branch have testified repeatedly on the need to reauthorize the Act. Since September, I have testified on this issue before the Senate Intelligence Committee, the House Permanent Select Committee on Intelligence, and the House Judiciary Committee. Officials of the Executive Branch also have participated in numerous other meetings with Members and staff on this important topic.

In the Senate, this valuable process has culminated in the strong bipartisan bill referred to this Committee, S. 2248, and we applaud Congress for its initiative on this issue and its willingness to consult with us as it moves forward on FISA modernization. I am happy to be here today to continue the public discussion on this topic, and I look forward to working with this Committee as it considers S. 2248.

We still are reviewing S. 2248, which was voted out of committee on a bipartisan 13-2 vote two weeks ago, but we believe it is a balanced bill that includes many sound provisions that would allow our Intelligence Community to continue obtaining the information it needs to protect the nation. We therefore are optimistic that S. 2248 will lead to a bill the President can sign. We do, however, have concerns with certain provisions in S. 2248 and we look forward to working with this Committee and Congress to address those concerns and achieve lasting FISA reform.

In my testimony today, I will briefly summarize the primary reasons that FISA needs to be modernized, and I will explain how we have implemented the Protect America Act. I also will discuss our views on certain provisions of The FISA Amendments Act of 2007 (S. 2248)

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00150 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.091

and explain why that bill is superior to H.R. 3773. While we appreciate the work of the House of Representatives in holding hearings and considering the challenges posed by the outdated provisions of FISA, H.R. 3773 is problematic in several respects, and if that bill is presented to the President in its current form, his senior advisers and the DNI will recommend that he veto it.

The Need for Permanent FISA Modernization

To understand why FISA needs to be modernized, it is important to understand some of the historical background regarding the statute. Congress enacted FISA in 1978 for the purpose of establishing a "statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes." H.R. Rep. No. 95-1283, pt. 1, at 22 (1978). The law authorized the Attorney General to make an application to a newly established court—the Foreign Intelligence Surveillance Court (or "FISA Court")—seeking a court order approving the use of "electronic surveillance" against foreign powers or their agents.

FISA established a regime of judicial review for foreign intelligence surveillance activities—but not for all such activities; only for certain of those that most substantially implicated the privacy interests of people in the United States. Congress designed a judicial review process that would apply primarily to surveillance activities within the United States—where privacy interests are the most pronounced—and not to overseas surveillance against foreign intelligence targets—where cognizable privacy interests are minimal or non-existent. The intent of Congress generally to exclude these intelligence activities from FISA's reach is expressed clearly in the House Permanent Select Committee on Intelligence's report, which explained: "[t]he committee has explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances." *Id.* at 27.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00151 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.092

As a result of changes in telecommunications technology since 1978, however, the scope of activities covered by FISA expanded—without any conscious choice by Congress—to cover a wide range of intelligence activities that Congress intended to exclude from FISA in 1978. This unintended expansion of FISA's scope hampered our intelligence capabilities and caused us to expend resources on obtaining court approval to conduct intelligence activities directed at foreign persons overseas. Prior to the passage of the Protect America Act of 2007, the Government often needed to obtain a court order before intelligence collection could begin against a target located overseas. Thus, considerable resources of the Executive Branch and the FISA Court were being expended on obtaining court orders to monitor the communications of terrorist suspects and other national security threats abroad. This effectively was granting constitutional protections to these foreign terrorist suspects, who frequently are communicating with other persons outside the United States.

In certain cases, this requirement of obtaining a court order slowed, and in some cases may have blocked, the Government's efforts to conduct surveillance of communications that were potentially vital to the national security. This expansion of FISA's reach also necessarily diverted resources that would have been better spent on protecting the privacy interests of United States persons here in the United States.

The Protect America Act of 2007

To address this and other problems and deficiencies in the FISA statute, the Administration submitted its FISA modernization proposal to Congress this April. Although Congress has yet to conclude its consideration of the Administration's proposal, you took a significant step in the right direction by passing the Protect America Act in August. By updating the definition of "electronic surveillance" to exclude surveillance directed at persons reasonably

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00152 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.093

believed to be outside the United States, the Protect America Act amended FISA to exclude from its scope those acquisitions directed at foreign intelligence targets located in foreign countries. This law has temporarily restored FISA to its original, core purpose of protecting the rights and liberties of people in the United States, and the Act allows the Government to collect the foreign intelligence information necessary to protect our nation. The passage of the Protect America Act represented the right policy solution—allowing our intelligence agencies to surveil foreign intelligence targets located outside the United States without prior court approval—and one that is consistent with our Constitution.

(1) Our Use of this New Authority

Our experience since the passage of the Protect America Act has demonstrated the critical need to reauthorize the Act's core authorities and we urge Congress to make those provisions permanent. Prior to the passage of the Act, the Director of National Intelligence testified that the Intelligence Community was unable to obtain the foreign intelligence information, including information from terrorist communications, that it needed to collect in a timely manner in order to protect Americans from national security threats.

The authority provided by the Protect America Act has allowed us temporarily to close intelligence gaps that were caused by FISA's outdated provisions. I understand that since the passage of the Act, the Intelligence Community has collected critical intelligence important to preventing terrorist actions and enhancing our national security. The Intelligence Community needs to be able to continue to effectively obtain information of this nature if we are to stay a step ahead of terrorists who want to attack the United States, and Congress should make the core provisions of the Protect America Act permanent.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00153 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.094

(2) Oversight of the PAA Authority

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

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

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

(3) Congressional Reporting About Our Use of the PAA Authority

We also are reporting to Congress about our implementation and use of this new authority in a manner that goes well beyond the reporting required by the Act. The Act provides that the Attorney General shall report on acquisitions under section 105B on a semiannual basis to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on the Judiciary of the Senate and of the House of Representatives. This report must include incidents of non-compliance with

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00154 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.095

the procedures used to determine whether a person is reasonably believed to be located outside the United States, non-compliance by a recipient of a directive, and the number of certifications issued during the reporting period.

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

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

We already have provided the Committee with documents related to our implementation of this new authority and have briefed appropriately cleared Committee staff members on PAA implementation issues. We also have completed several compliance reviews and are prepared to brief you on those reviews whenever it is convenient for you. Agencies employing this authority also continue to conduct on-site briefings, where Members and appropriately cleared staff have the opportunity to see how the Act has been implemented and to ask questions of those in the front lines of using this authority.

I am confident that this regime of oversight and congressional reporting will demonstrate

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00155 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.096

that we are effectively using this new authority to defend our country while assiduously protecting the civil liberties and privacy interests of Americans.

S. 2248: The FISA Amendments Act of 2007

As you know, the Senate Select Committee on Intelligence voted a bill out of committee two weeks ago with strong bipartisan support, and we are continuing to review that bill—The FISA Amendments Act of 2007 (S. 2248). We believe the bill is generally a strong piece of legislation, and that it includes a number of important revisions to FISA.

(1) Core Collection Authority

First, like the PAA, S. 2248 would allow our intelligence professionals to collect foreign intelligence against targets located outside the United States without obtaining prior court approval. This represents the same fundamental policy judgment underlying the Protect America Act—that our intelligence agencies should be able to collect foreign intelligence on targets located outside the United States without prior court approval. It has been clear throughout this process that there is a general consensus that the Government should not be required to obtain a court order to acquire foreign intelligence on targets located abroad, and we strongly support reauthorization of the authority to collect intelligence on targets located outside the United States without prior court approval.

(2) Retroactive Immunity

Second, section 202 of S. 2248 would afford retroactive immunity from private lawsuits for those companies alleged to have assisted the Government in the aftermath of the September 11th attacks. Electronic communication service providers ("providers") have faced numerous lawsuits as a result of their alleged activities in support of the Government's efforts to prevent another terrorist attack. It is imperative that this provision be retained in this bill.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00156 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.097

We believe that this is a just result. Any company that assisted the Government in defending our national security deserves our gratitude, not an avalanche of lawsuits. As the Senate Intelligence Committee noted in its report, the pending suits "seek hundreds of billions of dollars in damages from electronic communication service providers." S. Rep. No. 110-209, at 8 (2007) (hereinafter "Sen. Rep."). Under the proposal, a judge would dismiss a suit only if one of two circumstances is met: (1) the alleged assistance was not provided; or (2) the alleged assistance was in connection with an intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; was designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and was described in a written request or directive from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was authorized by the President and determined to be lawful. S. 2248, § 202.

After reviewing the relevant documents, and without identifying either the specific companies or the activities for which the companies provided assistance, the Intelligence Committee concluded that the providers had acted in response to written requests or directives stating that the activities had been authorized by the President and had been determined to be lawful. Sen. Rep. at 10. Because the committee "concluded that the providers . . . had a good faith basis for responding to the requests for assistance they received," *id.* at 11, the committee concluded that the providers "should be entitled to protection from civil suit." *Id.* The committee's considered judgment reflects a principle in the common law that private citizens who respond, in good faith, to a request for assistance by public officials should not be held liable for their actions.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00157 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.098

In addition to being the just outcome, providing this litigation protection is important to the national security. Companies in the future may be less willing to assist the Government if they face litigation each time they are alleged to have provided assistance. As the Intelligence Committee noted in its report, "electronic communication service providers play an important role in assisting intelligence officials in national security activities. Indeed, the intelligence community cannot obtain the intelligence it needs without assistance from these companies." *Id.* Because of the need for such cooperation in the future and the extent of the lawsuits that have been filed, that committee concluded that retroactive immunity was a necessity.

> Given the scope of the civil damages suits, and the current spotlight associated with providing any assistance to the intelligence community, the Committee was concerned that, without retroactive immunity, the private sector might be unwilling to cooperate with lawful Government requests in the future without unnecessary court involvement and protracted litigation. *The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation.*

Id (emphasis added). We are encouraged by that committee's recognition that retroactive immunity is necessary to ensure timely cooperation from providers.

Further, allowing continued litigation also risks the disclosure of highly classified information regarding intelligence sources and methods. The Intelligence Committee recognized in its report that this information should not be disclosed publicly.

> [T]he identities of persons or entities who provide assistance to the U.S. Government are protected as vital sources and methods of intelligence. . . . It would inappropriate to disclose the names of the electronic communication service providers from which assistance was sought, the activities in which the Government was engaged or in which providers assisted, or the details regarding any such assistance.

Sen. Rep. at 10. Our adversaries can be expected to use such information to their benefit, and we should not allow them to benefit from this needless litigation. The prevention of such disclosures also is important to the security of the facilities and personnel of relevant electronic

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00158 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.099

communication service providers. The retroactive immunity provision in S. 2248 would ensure that cases against private entities falling within its terms will be dismissed and would help prevent the disclosure of highly classified information.

The Intelligence Committee's decision to provide retroactive immunity to electronic communication service providers also reflects a recognition that indemnification—whereby the Government would be responsible for any damages awarded against the providers—is not a workable response to the extensive litigation these companies face. First, even if they receive indemnification, the relevant companies would still face the burden of litigation. After all, they would still be parties to the lawsuits, and all of the potential litigation burdens would still fall on them as parties. Second, even if they would no longer face the possibility of an award of damages, the relevant companies could suffer damage to their business reputations and stock prices as a result of such litigation. Finally, as discussed above, allowing these cases to continue risks the further disclosure of highly classified information regarding intelligence sources and methods.

Similarly, substitution—whereby the Government would litigate in place of the electronic communication service providers—is not a workable solution. Although the providers would no longer be parties to the litigation, in order to prove their claims, the plaintiffs in these cases will certainly continue to seek discovery (through document requests, depositions, and similar means) from the providers. Thus, like indemnification, substitution would still place a burden of discovery on the companies, risk damaging their business reputations and stock prices, and risk the disclosure of highly classified information. Moreover, both indemnification and substitution could result in a tremendous waste of taxpayer resources on these lawsuits.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00159 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.100

The Intelligence Committee's decision to include retroactive immunity in the bill reflects a recognition that retroactive immunity is the best solution to the extensive litigation faced by the relevant companies. Indeed, the Committee rejected an amendment to strike Title II of the bill, which includes the immunity provision, on a 12-3 vote, and it is imperative that this provision be retained in the bill.

(3) Other Provisions Related to Litigation

Third, the bill contains several other beneficial provisions related to litigation and state investigations. Section 203 of S. 2248 provides a "procedure that can be used in the future to seek dismissal of a suit when a defendant either provided assistance pursuant to a lawful statutory requirement, or did not provide assistance." Sen. Rep. at 12. As the Intelligence Committee noted, where a defendant has provided assistance to the Government pursuant to a lawful statutory requirement, but it would harm the national security for the request or assistance to be disclosed, such a procedure is a logical and expeditious way to achieve dismissal of such cases in the future. *Id.* In addition, section 204 of the bill would preempt state investigations or required disclosures of information—another important step in protecting highly classified information regarding classified sources and methods.

(4) Streamlining Provisions

Finally, sections 104 through 108 of S. 2248 would streamline the FISA application process in several positive ways. While FISA should require the Government, when applying for a FISA Court order, to provide information necessary to establish probable cause and other essential FISA requirements, FISA today requires the Government to provide information that is not necessary to these objectives. Among other things, the relevant sections of S. 2248 would eliminate unnecessary paperwork, while ensuring that the FISA Court has the information it

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00160 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.101

needs to process applications. As the Intelligence Committee stated in its report, these changes generally "are intended to increase the efficiency of the FISA process without depriving the Foreign Intelligence Surveillance Court of the information it needs to make findings required under FISA." Sen. Rep. at 21.

Those sections also would make other improvements to FISA, such as increasing the time the Government has to file an application for a court order after authorizing emergency surveillance. Currently the Executive Branch has 72 hours to obtain court approval after emergency surveillance is initially authorized by the Attorney General. S. 2248 would extend the emergency period to seven days. This change will help ensure that the Executive Branch has sufficient time in an emergency situation to accurately prepare an application, obtain the required approvals of senior officials, apply for a court order, and satisfy the court that the application should be granted. While we are encouraged by the progress that has been made on reauthorization of the Protect America Act authorities, we still have concerns with certain provisions of S. 2248.

(5) United States Persons Located Outside the United States

First, we strongly oppose proposed subsection 703(c) of that bill, which would introduce a new role for the FISA Court with respect to collecting intelligence from United States persons located outside the United States.

It is unwise to extend this new role to the FISA Court. Traditionally, surveillance of United States persons overseas has been regulated by a time-tested Executive Branch process under Executive Order 12333. That executive order requires the Attorney General to make an individualized probable cause determination before the Government may conduct foreign intelligence surveillance on a United States person overseas. Prior to authorizing the use of such

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00161 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.102

techniques, the Attorney General must determine that there is probable cause to believe that the United States person being targeted is a "foreign power" or "agent of a foreign power." These procedures, which have successfully balanced Americans' privacy interests with the national security for over 25 years, were unchanged by the Protect America Act.

It would be a significant departure to extend the role of the FISA Court and require the Government to obtain the approval of the court to collect foreign intelligence regarding United States persons overseas. The Government is not required to obtain a warrant to collect evidence outside the United States when its purpose is to build a criminal case—where the expected end of the investigative process is often the criminal prosecution of that United States person. It makes little sense to create a court approval requirement in the context of foreign intelligence collection—when the objective is the defense of our national security and operational flexibility and speed are critical to achieve that objective. Congress did not create this role for the FISA Court when it enacted FISA in 1978, and it should not extend the court's role in that regard in this legislation.

Subsection 703(c) of S. 2248, which would require the Attorney General to submit an application to the FISA Court to conduct an acquisition targeting a United States person overseas and to obtain a court order approving the acquisition prior to initiating it, also could have unintended consequences. First, unlike the current provisions of FISA governing electronic surveillance and physical searches, subsection 703(c) does not allow acquisitions regarding United States persons overseas to begin before obtaining court approval in emergency situations. Without an emergency provision, this subsection could impede operations and would result in the anomalous situation that it would be more difficult to surveil a United States person outside the country than inside the country. Second, extending this new role to the FISA Court and

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00162 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.103

requiring the court to approve acquisitions abroad could cause that court to feel compelled to analyze questions of foreign law as they relate to acquisitions under subsection 703(c), which could significantly complicate these types of collections and inject unpredictability into the process. We look forward to working with the Congress on this subsection as it considers S. 2248.

6. Sunset Provision

We also are opposed to the sunset provision in S. 2248 (section 101(c)), which would cause important provisions of the bill to sunset on December 31, 2013. In certain circumstances, a sunset provision may make sense. Where Congress enacts significant changes to existing legal authorities without the opportunity for sufficient deliberation or fact-finding, a sunset provision can afford Congress the chance to evaluate the effect of certain legislation. For example, the PATRIOT Act, which was enacted very quickly after the September 11th attacks, included sunset provisions and we recognize why Congress chose to include sunset provisions in that legislation. We also understand why Congress chose to include a sunset provision in the Protect America Act, which was similarly passed in response to a compelling and immediate need.

In contrast, a sunset provision should not be included in S. 2248, which would reauthorize the core authorities Congress included in the Protect America Act. There has been extensive public discussion and consideration of FISA modernization and the Protect America Act, both before and after passage of that Act in August. There is now a lengthy factual record on the need for FISA modernization, the implementation of the Protect America Act, the implications of the core authorities under the Act, and the appropriate level of Congressional oversight of this authority. Executive Branch officials have testified at numerous hearings over the last two years and conducted countless briefings for Members and staff on the need for FISA

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00163 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.104

modernization and the implementation of the Protect America Act. In addition, the Executive Branch has provided Congress with extensive information regarding the implementation of the Act—information that went well beyond that required by the statute. This has provided a track record of our implementation of the Protect America Act authority and has afforded Congress the opportunity to study this issue extensively. As the Intelligence Committee explained, S. 2248 reflects the culmination of a long process of hearings, classified briefings, and the review of relevant documents. S. Rep. at 2-3. Given the extensive factual record and public debate on these issues, the sunset provision in S. 2248 is not necessary.

We oppose the sunset provision because it introduces a significant level of uncertainty to the rules employed by our intelligence professionals and followed by our private partners. It is inefficient and unworkable for agencies to develop new processes and procedures and train their employees, only to have the law change within a period of several years. The Intelligence Community operates much more effectively when the rules governing our intelligence professionals' ability to track our enemies are established and are not in a persistent state of doubt.

7. Reporting and Oversight Provisions

We are continuing to analyze the increased reporting and oversight requirements in S. 2248 to determine whether they strike a workable balance between Congress's need for information concerning intelligence activities and the dedication of resources necessary to meet those reporting requirements. We value Congressional oversight of the Protect America Act authorities and we understand that oversight is necessary to demonstrate publicly that we are employing the authorities responsibly, as was made clear by our decision to exceed substantially the Congressional reporting requirements under the Act.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00164 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.105

We are, however, troubled by certain provisions of S. 2248, which may pose significant burdens on our intelligence agencies. For example, subsection 703(l) requires, among other things, an annual review to determine "the number of persons located in the United States whose communications were reviewed." S. 2248, § 703(l). Given the fragmentary nature of foreign intelligence collection and the limited amount of information available concerning any specific intercepted communication, I am informed that it would likely be impossible for intelligence agencies to comply with this requirement.

H.R. 3773

In contrast to S. 2248, the legislation introduced in the House of Representatives—H.R. 3773—falls short of providing the Intelligence Community with the tools it needs to collect foreign intelligence effectively from individuals located outside the United States. While we appreciate the efforts of the House to introduce a bill on this topic, we believe H.R. 3773 would be a step backward for national security. As the Administration has stated, if H.R. 3773 is presented in its current form to the President, the Director of National Intelligence and the President's other senior advisers will recommend that he veto the bill.

H.R. 3773 is deficient in several respects. First, it would limit the type of foreign intelligence information that could be acquired under its authority. Since 1978, FISA has provided for the collection of foreign intelligence information, and there is no reason to place complex restrictions on the types of intelligence that can be collected from persons outside the United States under this authority. This limitation would serve only to require intelligence analysts to spend valuable time and resources in distinguishing between types of foreign intelligence information being collected.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00165 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.106

Second, H.R. 3773 does not provide retroactive liability protection to electronic communication service providers or federal preemption of state investigations. As discussed above and recognized by the Senate Intelligence Committee in its report, those companies alleged to have assisted the Government in the aftermath of September 11th should not face litigation over those matters. Such litigation risks the disclosure of highly classified information and could lead to reduced intelligence collection capabilities in the future by discouraging companies from cooperating with the Government.

Third, in contrast to the Protect America Act and S. 2248, H.R. 3773 would require prior court approval for acquisitions of foreign intelligence information on targets located overseas absent an emergency. This is a significant increase in the role of the FISA Court with respect to the authorities provided by the Act and it could impede the collection of necessary foreign intelligence information. In addition, these provisions would not provide any meaningful increase in the protection of the privacy interests of Americans in the United States. H.R. 3773 also fails explicitly to provide for continued intelligence collection while the Government appeals an order of the FISA Court.

Finally, H.R. 3773 would sunset in a little over two years. As discussed above, intelligence agencies need certainty and permanence in the rules they employ for intelligence collection and we oppose any sunset provision. We are strongly opposed to the extremely short sunset provision in H.R. 3773.

While we look forward to working with Congress towards the passage of a permanent FISA modernization bill that would strengthen the Nation's intelligence capabilities while respecting the constitutional rights of Americans, we cannot support H.R. 3773 in its current form.

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00166 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.107

Conclusion

The Protect America Act has been critical to our efforts to gather the foreign intelligence information necessary to protect the Nation, and it is crucial that its core aspects be made permanent. In addition to making the core provisions of the Protect America Act permanent, Congress should reform FISA in accordance with the other provisions in the proposal that the Administration submitted to the Congress in April. It is especially imperative that Congress provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities in the wake of the September 11 attacks. These changes would permanently restore FISA to its original focus on the protection of the privacy interests of Americans, improve our intelligence capabilities, and ensure that scarce Executive Branch and judicial resources are devoted to the oversight of intelligence activities that most clearly implicate the interests of Americans. We are encouraged by the progress that has been made on this issue, particularly with respect to many of the provisions in S. 2248, and we look forward to working with Congress and this Committee as it considers S. 2248.

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

VerDate Nov 24 2008 11:52 Oct 06, 2009 Jkt 052426 PO 00000 Frm 00167 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\52426.TXT SJUD1 PsN: CMORC

52426.108

Surveillance Sanity

By BENJAMIN CIVILETTI, DICK THORNBURGH and WILLIAM WEBSTER
October 31, 2007; Page A21

Following the terrorist attacks of Sept. 11, 2001, President Bush authorized the National Security Agency to target al Qaeda communications into and out of the country. Mr. Bush concluded that this was essential for protecting the country, that using the Foreign Intelligence Surveillance Act would not permit the necessary speed and agility, and that he had the constitutional power to authorize such surveillance without court orders to defend the country.

Since the program became public in 2006, Congress has been asserting appropriate oversight. Few of those who learned the details of the program have criticized its necessity. Instead, critics argued that if the president found FISA inadequate, he should have gone to Congress and gotten the changes necessary to allow the program to proceed under court orders. That process is now underway. The administration has brought the program under FISA, and the Senate Intelligence Committee recently reported out a bill with a strong bipartisan majority of 13-2, that would make the changes to FISA needed for the program to continue. This bill is now being considered by the Senate Judiciary Committee.

Public disclosure of the NSA program also brought a flood of class-action lawsuits seeking to impose massive liability on phone companies for allegedly answering the government's call for help. The Intelligence Committee has reviewed the program and has concluded that the companies deserve targeted protection from these suits. The protection would extend only to activities undertaken after 9/11 until the beginning of 2007, authorized by the president to defend the country from further terrorist attack, and pursuant to written assurances from the government that the activities were both authorized by the president and legal.

We agree with the committee. Dragging phone companies through protracted litigation would not only be unfair, but it would deter other companies and private citizens from responding in terrorist emergencies whenever there may be uncertainty or legal risk.

The government alone cannot protect us from the threats we face today. We must have the help of all our citizens. There will be times when the lives of thousands of Americans will depend on whether corporations such as airlines or banks are willing to lend assistance. If we do not treat companies fairly when they respond to assurances from the highest levels of the government that their help is legal and essential for saving lives, then we will be radically reducing our society's capacity to defend itself.

This concern is particularly acute for our nation's telecommunications companies. America's front line of defense against terrorist attack is communications intelligence. When Americans put their loved ones on planes, send their children to school, or ride through tunnels and over bridges, they are counting on the "early warning" system of communications intelligence for their safety. Communications technology has become so complex that our country needs the voluntary cooperation of the companies. Without it, our intelligence efforts will be gravely damaged.

52426.109

Whether the government has acted properly is a different question from whether a private person has acted properly in responding to the government's call for help. From its earliest days, the common law recognized that when a public official calls on a citizen to help protect the community in an emergency, the person has a duty to help and should be immune from being hauled into court unless it was clear beyond doubt that the public official was acting illegally. Because a private person cannot have all the information necessary to assess the propriety of the government's actions, he must be able to rely on official assurances about need and legality. Immunity is designed to avoid the burden of protracted litigation, because the prospect of such litigation itself is enough to deter citizens from providing critically needed assistance.

As the Intelligence Committee found, the companies clearly acted in "good faith." The situation is one in which immunity has traditionally been applied, and thus protection from this litigation is justified.

First, the circumstances clearly showed that there was a bona fide threat to "national security." We had suffered the most devastating attacks in our history, and Congress had declared the attacks "continue to pose an unusual and extraordinary threat" to the country. It would have been entirely reasonable for the companies to credit government representations that the nation faced grave and immediate threat and that their help was needed to protect American lives.

Second, the bill's protections only apply if assistance was given in response to the president's personal authorization, communicated in writing along with assurances of legality. That is more than is required by FISA, which contains a safe-harbor authorizing assistance based solely on a certification by the attorney general, his designee, or a host of more junior law enforcement officials that no warrant is required.

Third, the ultimate legal issue -- whether the president was acting within his constitutional powers -- is not the kind of question a private party can definitively determine. The companies were not in a position to say that the government was definitely wrong.

Prior to FISA's 1978 enactment, numerous federal courts took it for granted that the president has constitutional power to conduct warrantless surveillance to protect the nation's security. In 2002, the FISA Court of Review, while not dealing directly with the NSA program, stated that FISA could not limit the president's constitutional powers. Given this, it cannot be said that the companies acted in bad faith in relying on the government's assurances of legality.

For hundreds of years our legal system has operated under the premise that, in a public emergency, we want private citizens to respond to the government's call for help unless the citizen knows for sure that the government is acting illegally. If Congress does not act now, it would be basically saying that private citizens should only help when they are absolutely certain that all the government's actions are legal. Given the threats we face in today's world, this would be a perilous policy.

Mr. Civiletti was U.S. attorney general under President Jimmy Carter, Mr. Thornburgh was U.S. attorney general under President George H.W. Bush and Judge Webster is former director of the CIA and former director of the FBI.

52426.110