



U.S. Department of Justice

Office of Information and Privacy

Telephone: (202) 514-3642

Washington, D.C. 20530

APR 21 2008

Ms. Marcia Hofmann
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Re: AG/08-R0183
OLA/08-R0184
OLP/08-R0185
MAP:TEH:NDD

Dear Ms. Hofmann:

This is our final response to your Freedom of Information Act (FOIA) requests dated December 21, 2007, which were received in this Office on December 27, 2007, in which you requested all records of communications between the Department of Justice and Members of Congress and between the Department and telecommunications companies from September 1, 2007, to the present concerning amendments to the Foreign Intelligence Surveillance Act. This response is made on behalf of the Offices of the Attorney General, Legal Policy (OLP) and Legislative Affairs (OLA).

We have located seventy documents, totaling 535 pages, that are responsive to your request. One of these documents, totaling five pages, was released to you by our memorandum dated April 3, 2008. With regard to the remaining documents, I have determined that fifty-two documents, totaling 293 pages, are appropriate for release without excision and copies are enclosed. Of these documents, five had portions that did not consist of exchanges between the Department and Members of Congress or representatives of telecommunications companies regarding amendments to the Foreign Intelligence Surveillance Act. We have removed the non-responsive material, and provided the responsive portions of these documents without excision. Please note, with regard to document number OAG-2, a total of fifty-eight pages were not provided to you, as the material did not concern amendments to the Foreign Intelligence Surveillance Act.

I have determined that the responsive portion of document number OLA-90, totaling two pages, is appropriate for release with excisions made on behalf of the Office of the Director of National Intelligence (ODNI) pursuant to Exemption 2 of the FOIA, 5 U.S.C. § 552(b)(2), which pertains to purely internal agency practices. Additionally, one document, number OAG-22, totaling one page, is appropriate for release with an excision made on behalf of the Department of Justice Office of Legal Counsel (OLC) pursuant to Exemption 5 of the FOIA, 5 U.S.C. § 552(b)(5), which pertains to certain inter- and intra-agency communications protected by the deliberative process privilege.

Additionally, one document, totaling two pages, contains responsive portions that are being withheld in full pursuant to Exemption 5 of the FOIA, 5 U.S.C. § 552(b)(5), which pertains to certain inter- and intra-agency communications protected by the deliberative process privilege.

For your information, this document consists of electronic mail (e-mail messages) in which Department of Justice officials discuss the positions certain senators have taken on proposed amendments to the Foreign Intelligence Surveillance Act.

Please also be advised that fourteen documents, totaling 174 pages, were referred to other Department of Justice components or other government entities for processing and direct response to you. Specifically, within the Department of Justice, three documents, totaling nine pages, were referred to the Civil Division, six documents, totaling 141 pages, were referred to the National Security Division (NSD), and two classified documents, totaling fifteen pages, were referred to the Federal Bureau of Investigation. Furthermore, three documents, totaling nine pages, were referred to the Office of the Director of National Intelligence (ODNI).

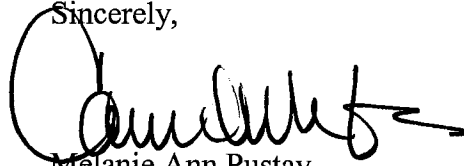
While processing its own FOIA request from you, NSD referred a total of nine documents, totaling thirty-two pages, and OLC referred, through NSD, one classified document totaling three pages, to this Office for processing and direct response to you. Upon review, we determined that seven of these documents, totaling twenty-eight pages, were duplicates of documents that we were already processing pursuant to your request to this Office. Accordingly, we did not process those seven documents referred by NSD. With regard to the remaining three documents, totaling seven pages, I have determined that two documents, totaling four pages, are appropriate for release without excision and copies are enclosed. The final document, totaling three pages, is being released to you in part, with excisions made on behalf of NSD pursuant to Exemptions 1 and 3 of the FOIA, 5 U.S.C. § 552(b)(1) and 3, which pertain to information that is properly classified in the interest of national security pursuant to Executive Order 12958, as amended, and to information exempted from release by statute, in this instance 50 U.S.C § 403-1(i), 18 U.S.C. § 798, and 50 U.S.C. § 402 note, which pertain to the protection of intelligence sources and methods from unauthorized disclosure, protection of information concerning the nature, preparation, or use of any code, cipher or cryptographic system of the United States from unauthorized disclosure, and the organization, functions, activities, and personnel of the National Security Agency.

Finally, while processing its own FOIA request from you, ODNI referred one e-mail chain, totaling one page, to this Office for processing and direct response to you. This document is being withheld in full pursuant to Exemption 5 of the FOIA, 5 U.S.C § 552 (b)(5), which pertains to certain inter- and intra-agency communications protected by the presidential communications privilege. For your information, the e-mail contains information from a Department of Justice official written to several White House officials providing a candid analysis of, and comments on, a briefing given to certain Members of Congress regarding amendments to the Foreign Intelligence Surveillance Act.

Also, as you may already be aware, the Department has made and continues to make certain documents pertaining to potential amendments to the Foreign Intelligence Surveillance Act available on its web site at <http://www.lifeandliberty.gov/>.

Although I am aware that your request is the subject of ongoing litigation and that appeals are not ordinarily acted on in such situations, I am required by statute and regulation to inform you that you have the right to file an administrative appeal.

Sincerely,

A handwritten signature in black ink, appearing to read "Melanie Ann Pustay", with a long horizontal flourish extending to the right.

Melanie Ann Pustay
Director

Enclosures

JOHN CONYERS, JR., Michigan
CHAIRMAN

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

LAMAR S. SMITH, Texas
RANKING MINORITY MEMBER

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

ONE HUNDRED TENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6216

(202) 225-3951

<http://www.house.gov/judiciary>

September 12, 2007

The Honorable Kenneth Wainstein
Assistant Attorney General for National Security
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Mr. Wainstein:

The House Committee on the Judiciary will hold a hearing on Tuesday, September 18, 2007, at 11:00 a.m. in room 2141 Rayburn House Office Building. The hearing is on Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights.

I would like to invite you to testify at this hearing. Please prepare a written statement for submission to the Committee prior to your appearance. The written statement may be as extensive as you wish and will be included in the hearing record. To allow sufficient time for questions at the hearing, please briefly highlight the most significant points of the written statement in an oral presentation lasting five minutes or less. Oral testimony at the hearing, including answers to questions, will be printed as part of the verbatim record of the hearing. Only transcription errors may be edited subsequent to the hearing.

To facilitate preparation for the hearing, please send an electronic copy of your written statement and curriculum vitae to the Committee 48 hours in advance of the hearing. The Committee will publish the statement on our website and, therefore, requests that you provide the documents in Word Perfect, Microsoft Word, or Adobe Acrobat. Please number all pages of the written statement, and attach a cover page with your name, position, date, and the title of the hearing. These documents may be e-mailed to Lou DeBaca on my staff at Lou.DeBaca@mail.house.gov.

ES-1

The Honorable Kenneth Wainstein
Page Two
September 12, 2007

In addition, the Committee requests that you provide 50 copies of your written statement to Lou DeBaca, 2138 Rayburn House Office Building, Washington, DC, 20515, 48 hours in advance of the hearing. Due to delays with our current mail delivery system, the copies should be hand delivered in an unsealed package. If this is not possible, please bring the copies with you the day of the hearing. Should you intend to introduce a published document or report as part of your written statement, I ask that you provide 60 copies for the hearing. Should such material be available on the Internet, please prepare a page containing citations to such material and provide the Committee with 50 copies.

If you have any questions or concerns, please contact Lou DeBaca on my staff at 202-225-3951.

I look forward to your participation in the hearing.

Sincerely,

A handwritten signature in black ink, appearing to read "John Conyers, Jr.", written in a cursive style.

John Conyers, Jr.
Chairman



U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 24, 2007

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

Dear Mr. Chairman:

We understand that the Committee is holding a hearing tomorrow entitled, "Strengthening FISA-Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?" and that the Director of National Intelligence, J.M. McConnell, is scheduled to testify. We further understand that Director McConnell wrote to you suggesting that Assistant Attorney General Kenneth L. Wainstein appear as a co-witness with the Director.

The Department respects your prerogative as Chairman to structure Committee hearings in the manner that best addresses the Committee's need for information on critical issues like FISA modernization. Should you wish to hear from Mr. Wainstein at the hearing tomorrow, he stands ready and willing to testify. Moreover, we will remain ready to designate an appropriate witness to testify in the future if the Committee is interested in hearing from the Department of Justice on this critical legislation.

We appreciate the Committee's interest in this very important issue. Please do not hesitate to contact this office if we may be of assistance with this or any other matter.

Sincerely,

Brian A. Benczkowski
Principal Deputy Assistant Attorney General

cc: The Honorable Arlen Specter
Ranking Minority Member

ES-2

1275673
mrd

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

AILEN 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

United States Senate

COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-8275

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

October 18, 2007

Hon. Michael B. Mukasey
Patterson Belknap Webb & Tyler LLP
1133 Avenue of the Americas
New York, N.Y. 10036

Dear Judge Mukasey:

I appreciated your answers to my questions and to other Senators' questions at your hearing before the Senate Judiciary Committee. I will be following up with written questions on a number of important issues, but I wanted to highlight one issue on which it is particularly vital that you clarify your position as soon as possible.

You said in the context of warrantless surveillance that, despite Congress clearly having legislated in this area with the Foreign Intelligence Surveillance Act (FISA), the President may be able to act, and to authorize and immunize others to act, contrary to the clear boundaries of what the FISA law allows, because of the President's constitutional commander-in-chief powers.

However, you also said that, in the context of the use of torture or cruel, inhuman, or degrading treatment in the interrogation of detainees, the President could not authorize or immunize conduct outside of the law, even if he were to believe it would further his constitutional responsibility as commander-in-chief to do so.

You explained this distinction by saying that torture and cruel, inhuman, or degrading treatment are banned by the Constitution under the Fifth, Eighth, and Fourteenth Amendments, as well as by law. I find this distinction unhelpful because unreasonable search and seizure is much more clearly forbidden by the Constitution, in the Fourth Amendment, than torture or cruel, inhuman, and degrading treatment. In both situations, the President, in authorizing such conduct, would be flouting both statutory and constitutional prohibitions based on a broad assertion of executive power. I am concerned that this legal justification could lead to a continuation of the kind of warrantless surveillance in violation of statute that we have seen.

RECEIVED
OCT 18 10 11 5 19
EXECUTIVE SECRETARIAT

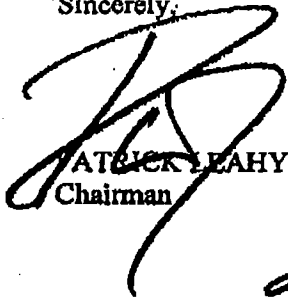
ES-4

Hon. Michael B. Mukasey
October 18, 2007
Page 2 of 2

Please clarify for me the distinction you are making and why your argument justifying presidential authority to authorize or immunize actions contrary to the FISA statute could not be similarly used to justify authorizing or immunizing action contrary to the statutory bans on torture and cruel, inhuman, or degrading treatment.

I look forward to your prompt answer.

Sincerely,



PATRICK LEAHY
Chairman

*I look forward to hearing
from you*

United States Senate

COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6276

Facsimile Cover Sheet

Please Deliver to: HON. PETER D. KEISLER

Fax No. 202-514-4507

From: CHAIRMAN LEAHY

Phone: 202-224-7703

Number of Pages Including Cover: 3

Comments:

If there are any problems with this transmission, please call: 224-7703

THE DOCUMENT TRANSMITTED IS CONFIDENTIAL AND INTENDED
FOR RECEIPT BY THE ABOVE NAMED INDIVIDUAL ONLY.

Michael B. Mukasey

October 24, 2007

The Honorable Patrick J. Leahy
United States Senate
Washington, D.C. 20510

Dear Chairman Leahy:

Thank you for the graciousness you and the other members of the Senate Judiciary Committee exhibited toward me throughout the hearing. Thank you also for your letter of October 18, which gives me the opportunity to address, again, some of the legal issues raised by foreign intelligence collection and interrogation practices.

As you point out, "torture is prohibited under the Fifth, Eighth, and Fourteenth Amendments, *as well as by law.*" (emphasis added) That coincides with what I said at the hearing, but the *as well as by law* part is important because the other law in this instance is a treaty, the United Nations Convention Against Torture and Cruel, Inhuman and Degrading Treatment (UNCAT), and legislation enacted to implement it that illuminate constitutional provisions.

When UNCAT was ratified in 1994, Congress complied with its terms by enacting statutes banning torture. Moreover, in consenting to ratification of the treaty, the Senate added the caveat that cruel, inhuman and degrading treatment would be understood in the United States as the treatment forbidden by the Fifth, Eighth and Fourteenth Amendments to the Constitution. Congress further extended the prohibition with the McCain Amendment (enacted as part of the Detainee Treatment Act in 2005), which statutorily bars cruel, inhuman and degrading treatment and reaffirms our treaty commitment. That amendment also extends the protection of those standards beyond the normal reach of the Constitution – as to both nationality and geography – to include aliens in the custody of the United States, wherever held, as does the implementing legislation banning torture.

Therefore, it is accurate to say that torture and cruel, inhuman and degrading treatment are prohibited by the laws of the United States, which of course includes the Constitution. Moreover, this protection, based as it is on a treaty and statutes enacted by Congress and signed by the President, is at the top of the three-tier hierarchy described by Justice Jackson in his famous concurrence in the Steel Seizure case. *Youngstown Sheet & Tube v. Sawyer*, 343 U.S. 579, 635-38 (1952) (Jackson, J., concurring). This status is enhanced further by the anti-torture reach of the referenced constitutional amendments.

ES-4A

Warrantless surveillance for the collection of foreign intelligence requires a different analysis. As an initial matter, it is widely accepted that the Constitution does not require that all searches be conducted pursuant to a warrant. The Supreme Court and the lower federal courts have upheld warrantless searches in numerous settings. Searches incident to arrest, border searches, and vehicle searches, to name a few examples, may be conducted without a warrant. Warrantless searches of this sort must still, of course, comply with the Fourth Amendment's reasonableness requirement. The federal courts have treated warrantless searches to obtain foreign intelligence analogously, holding that the Constitution does not require a warrant, although it does require that the searches be reasonable. See, e.g., *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973); see also *In re Sealed Case*, 310 F.3d 717, 742 (FIS Court of Review 2002).

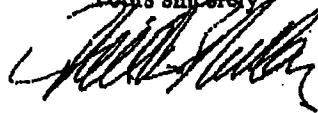
Accordingly, the weight of authority indicates that warrantless surveillance to collect foreign intelligence is not unconstitutional so long as it is otherwise reasonable. This is not to say the government may conduct such surveillance without regard for the privacy interests at stake. Warrantless surveillance directed at US individuals within the United States presents a more complex question, and understandably raises much greater concern, than surveillance directed at foreigners overseas. Indeed, the Foreign Intelligence Surveillance Act ("FISA") and the Protect America Act recognize this distinction and provide a greater role for the Foreign Intelligence Surveillance Court in reviewing and approving surveillance directed at people within the United States than people located abroad.

As I tried to stress during the hearing, government works best, and with the greatest legitimacy, when the branches act cooperatively, each with respect for the other's constitutional prerogatives. I agreed more than once that consultation between the Committee and the Department often can prevent issues from evolving into controversies. FISA appears to be a model of such cooperation and mutual respect. Thus, foreign intelligence gathering is a field in which the executive branch is regulated but not preempted by Congress. This approach has served us well.

As you noted, Congress has amended FISA several times at the request of the executive branch. To the extent FISA may be (or become) inadequate to the task of responding to threats we confront, it is imperative that the branches work together to amend the statute. I am not of the view that the President's constitutional authority to conduct the foreign affairs of the United States and protect our national security is inevitably in tension with Congress's power to legislate in those same areas. To the contrary, if confirmed, I would be a strong advocate for a cooperative approach to Congress in this and other matters of national security. During the hearing, I mentioned the danger of heedlessly carrying a principle off a cliff. There is no reason to provoke a constitutional controversy over a process that works well most of the time, that can be fixed where it does not work, and that involves the security of the American people.

I have no doubt that our country is best served when the political branches work in harmony to fulfill their shared responsibility of securing our Nation's safety from foreign threats. If confirmed, I intend to spend the time that remains for this Administration solving problems cooperatively with Congress rather than exploring our possible differences. I end where I began: I am grateful to you and the Committee for your graciousness.

Yours sincerely

A handwritten signature in black ink, appearing to read "Bill Clinton", written in a cursive style.

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*

United States Senate

COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6276

November 13, 2007

Bryan A. Benczkowski
Principle Deputy Assistant Attorney General
Office of Legislative Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Room 1601
Washington, DC 20530

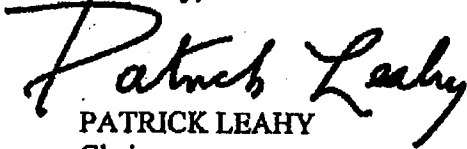
Dear Mr. Benczkowski:

Thank you for facilitating the testimony of Assistant Attorney General Kenneth L. Wainstein at the United States Senate Judiciary Committee hearing regarding "FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability" on October 31, 2007.

Enclosed are written questions from Committee members. In order to complete the hearing record, please send Mr. Wainstein's written responses as soon as possible and in no event later than Tuesday, November 27, 2007 to my office, attention Jennifer Price, Hearing Clerk, Senate Judiciary Committee, 224 Dirksen Senate Office Building, Washington, D.C., 20510. Please also send an electronic version of your responses to Jennifer_Price@judiciary-dem.senate.gov.

Again, thank you for your participation. If you have any questions, please contact Jennifer Price of my staff at (202) 224-7703.

Sincerely,


PATRICK LEAHY
Chairman

ES-5

**Senate Judiciary Committee Hearing on "FISA Amendments: How to Protect
Americans' Security and Privacy and Preserve the Rule of Law and Government
Accountability"**

Wednesday, October 31, 2007

**Questions Submitted by U.S. Senator Russell D. Feingold to Kenneth L. Wainstein
Assistant Attorney General**

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?
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?
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?
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?
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

ES-5B

but allowed the new definition of electronic surveillance in the Protect America Act to expire?

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?
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?
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?
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?
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?
 - b. Will you commit to announcing, publicly, the fact that such a petition has been filed?

Senator Edward M. Kennedy
Questions for the Record
Senate Judiciary Committee hearing on "FISA Amendments: How to Protect Americans'
Security and Privacy and Preserve the Rule of Law and Government Accountability"
Held on October 31, 2007

*To Kenneth L. Wainstein, Acting Attorney General, National Security Division, U.S.
Department of Justice*

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?
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 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?
- 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?

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?
2. If we do not extend the Protect America Act and do not pass any other new laws, will the Administration comply with FISA?
3. Are any electronic surveillance programs currently being conducted outside the authority of FISA as amended by the Protect America Act?
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?

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?
 - 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?
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?
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?
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?
 - a. If not, why not? Are you worried that courts will rule that the President's warrantless surveillance programs were illegal?
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, 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?

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.
- 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.
 - 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?
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?
 - 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?
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.
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?
 - 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.

**U.S. SENATE COMMITTEE ON THE JUDICIARY
FISA HEARING — OCTOBER 31, 2007
QUESTIONS FOR THE RECORD FOR MR. WAINSTEIN
SUBMITTED BY 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?

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?

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?

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?

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?

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 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 States. 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?

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?

**Questions of Senator Patrick J. Leahy
To Kenneth L. Wainstein**

Definition of "Electronic Surveillance"

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.

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?

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

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

Role of the FISA Court

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?

Immunity – Approval by Counsel to the President

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?

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?

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?

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*

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

October 25, 2007

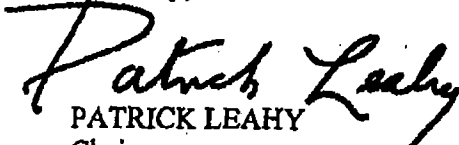
Bryan A. Benczkowski
Principle Deputy Assistant Attorney General
Office of Legislative Affairs
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Room 1601
Washington, DC 20530

Dear Mr. Benczkowski:

Thank you for facilitating Assistant Attorney General Kenneth L. Wainstein's appearance and testimony at the Senate Committee on the Judiciary hearing on "FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability" scheduled for Wednesday, October 31, 2007, at 10:00 a.m. in room 226 of the Dirksen Senate Office Building.

Committee rules require that that written testimony be provided by 10:00 a.m., Tuesday afternoon, October 30. Please provide 75 hard copies of the written testimony and curriculum vitae by that time. Send the hard copies as soon as possible to the attention of Jennifer Price, Hearing Clerk, Senate Committee on the Judiciary, 224 Dirksen Senate Office Building, Washington, D.C. 20510. Please also send electronic copy of the testimony and a short biography via email to Jennifer_Price@judiciary-dem.senate.gov.

Sincerely,


PATRICK LEAHY
Chairman

ES-6

February 5, 2008

The Honorable Harry Reid
Majority Leader
United States Senate
528 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Reid:

This letter presents the views of the Administration on various amendments to the Foreign Intelligence Surveillance Act of 1978 (FISA) Amendments Act of 2008 (S. 2248), a bill "to amend the Foreign Intelligence Surveillance Act of 1978, to modernize and streamline the provisions of that act, and for other purposes." The letter also addresses why it is critical that the authorities contained in the Protect America Act not be allowed to expire. We have appreciated the willingness of Congress to address the need to modernize FISA and to work with the Administration to allow the intelligence community to collect the foreign intelligence information necessary to protect the Nation while protecting the civil liberties of Americans. We commend Congress for the comprehensive approach that it has taken in considering these authorities and are grateful for the opportunity to engage with Congress as it conducts an in-depth analysis of the relevant issues.

In August, Congress took an important step toward modernizing FISA by enacting the Protect America Act of 2007. That Act has allowed us temporarily to close intelligence gaps by enabling our intelligence professionals to collect, without a court order, foreign intelligence information from targets overseas. The intelligence community has implemented the Protect America Act in a responsible way, subject to extensive executive branch, congressional, and judicial oversight, to meet the country's foreign intelligence needs while protecting civil liberties. Indeed, the Foreign Intelligence Surveillance Court (FISA Court) recently approved the procedures used by the Government under the Protect America Act to determine that targets are located overseas, not in the United States.

The Protect America Act was scheduled to expire on February 1, 2008, but Congress has extended that Act for fifteen days, through February 16, 2008. In the face of the continued threats to our Nation from terrorists and other foreign intelligence targets, it is vital that Congress not allow the core authorities of the Protect America Act to expire, but instead pass long-term FISA modernization legislation that both includes the collection authority conferred by the Protect America Act and provides protection from private lawsuits against companies that are believed to have assisted the Government in the aftermath of the September 11th terrorist attacks on America. Liability protection is the just result for companies who answered their Government's call for assistance. Further, it will ensure that the Government can continue to rely upon the assistance of the private sector that is so necessary to protect the Nation and enforce its laws.

ES-8

The Honorable Harry Reid

S. 2248, reported by the Senate Select Committee on Intelligence, would satisfy both of these imperatives. That bill was reported out of committee on a nearly unanimous 13-2 vote. Although it is not perfect, it contains many important provisions, and was developed through a thoughtful process that resulted in a bill that helps ensure that both the lives and the civil liberties of Americans will be safeguarded. First, it would establish a firm, long-term foundation for our intelligence community's efforts to track terrorists and other foreign intelligence targets located overseas. Second, S. 2248 would afford retroactive liability protection to communication service providers that are believed to have assisted the Government with intelligence activities in the aftermath of September 11th. In its report on S. 2248, the Intelligence Committee recognized 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." The committee's measured judgment reflects the principle that private citizens who respond in good faith to a request for assistance by public officials should not be held liable for their actions. Thus, with the inclusion of the proposed manager's amendment, which would make necessary technical changes to the bill, we strongly support passage of S. 2248.

For reasons elaborated below, the Administration also strongly favors two other proposed amendments to the Intelligence Committee's bill. One would strengthen S. 2248 by expanding FISA to permit court-authorized surveillance of international proliferators of weapons of mass destruction. The other would ensure the timely resolution of any challenges to government directives issued in support of foreign intelligence collection efforts.

Certain other amendments have been offered to S. 2248, however, that would undermine significantly the core authorities and immunity provisions of that bill. After careful study, we have determined that those amendments would result in a final bill that would not provide the intelligence community with the tools it needs to collect effectively foreign intelligence information vital for the security of the Nation. If the President is sent a bill that does not provide the U.S. intelligence agencies the tools they need to protect the nation, the President will veto the bill.

I. Limitations on the Collection of Foreign Intelligence

Several proposed amendments to S. 2248 would have a direct, adverse impact on our ability to collect effectively the foreign intelligence information necessary to protect the Nation. We note that three of these amendments were part of the Senate Judiciary Committee substitute, which has already been rejected by the Senate on a 60-34 vote. We explained why those three amendments were unacceptable in our November 14, 2007, letter to Senator Leahy regarding the Senate Judiciary Committee substitute, and the Administration reiterated these concerns in a Statement of Administration Policy (SAP) issued on December 17, 2007. A copy of that letter and the SAP are attached for your reference.

Prohibition on Collecting Vital Foreign Intelligence Information (No amendment number available). This amendment provides that "no communication shall be acquired under [Title VII of S. 2248] if the Government knows before or at the time of acquisition that the communication

The Honorable Harry Reid

is to or from a person reasonably believed to be located in the United States," except as authorized under Title I of FISA or certain other exceptions. The amendment would require the Government to "segregate or specifically designate" any such communication and the Government could access such communications only under the authorities in Title I of FISA or under certain exceptions. Even for communications falling under one of the limited exceptions or an emergency exception, the Government still would be required to submit a request to the FISA Court relating to such communications. The procedural mechanisms it would establish would diminish our ability swiftly to monitor a communication from a terrorist overseas to a person in the United States—precisely the communication that the intelligence community may have to act on immediately. Finally, the amendment would draw unnecessary and harmful distinctions between types of foreign intelligence information, allowing the Government to collect communications under Title VII from or to the United States that contain information relating to terrorism but not other types of foreign intelligence information, such as that relating to the national defense of the United States or attacks, hostile actions, and clandestine intelligence activities of a foreign power.

This amendment would eviscerate critical core authorities of the Protect America Act and S. 2248. Our prior letter and the Statement of Administration Policy explained how this type of amendment increases the danger to the Nation and returns the intelligence community to a pre-September 11th posture that was heavily criticized in congressional reviews. It would have a devastating impact on foreign intelligence surveillance operations; it is unsound as a matter of policy; its provisions would be inordinately difficult to implement; and thus it is unacceptable. The incidental collection of U.S. person communications is not a new issue for the intelligence community. For decades, the intelligence community has utilized minimization procedures to ensure that U.S. person information is properly handled and "minimized." It has never been the case that the mere fact that a person overseas happens to communicate with an American triggers a need for court approval. Indeed, if court approval were mandated in such circumstances, there would be grave operational consequences for the intelligence community's efforts to collect foreign intelligence. Accordingly, if this amendment is part of the bill that is presented to the President, we, as well as the President's other senior advisors, will recommend that he veto the bill.

Imposition of a "Significant Purpose" Test (No. 3913). This amendment, which was part of the Judiciary Committee substitute, would require an order from the Foreign Intelligence Surveillance Court (FISA Court) if a "significant purpose" of an acquisition targeting a person abroad is to acquire the communications of a specific person reasonably believed to be in the United States. If the concern driving this proposal is so-called "reverse targeting"—circumstances in which the Government would conduct surveillance of a person overseas when the Government's actual target is a person in the United States with whom the person overseas is communicating—that situation is already addressed in FISA today. If the person in the United States is the actual target, an order from the FISA Court is required. Indeed, S. 2248 codifies this longstanding Executive Branch interpretation of FISA.

The amendment would place an unnecessary and debilitating burden on our intelligence community's ability to conduct surveillance without enhancing the protection of the privacy of Americans. The introduction of this ambiguous "significant purpose" standard would raise

The Honorable Harry Reid

unacceptable operational uncertainties and problems, making it more difficult to collect intelligence when a foreign terrorist overseas is calling into the United States—which is precisely the communication we generally care most about. Part of the value of the Protect America Act, and any subsequent legislation, is to enable the intelligence community to collect expeditiously the communications of terrorists in foreign countries who may contact an associate in the United States. The intelligence community was heavily criticized by numerous reviews after September 11, including by the Congressional Joint Inquiry into September 11, regarding its insufficient attention to detecting communications indicating homeland attack plotting. To quote the Congressional Joint Inquiry:

The Joint Inquiry has learned that one of the future hijackers communicated with a known terrorist facility in the Middle East while he was living in the United States. The Intelligence Community did not identify the domestic origin of those communications prior to September 11, 2001 so that additional FBI investigative efforts could be coordinated. Despite this country's substantial advantages, there was insufficient focus on what many would have thought was among the most critically important kinds of terrorist-related communications, at least in terms of protecting the Homeland.

In addition, the proposed amendment would create uncertainty by focusing on whether the "significant purpose ... is to acquire the communication" of a person in the United States, not just to target the person here. To be clear, a "significant purpose" of intelligence community activities that target individuals outside the United States is to detect communications that may provide warning of homeland attacks, including communications between a terrorist overseas and associates in the United States. A provision that bars the intelligence community from collecting these communications is unacceptable. If this amendment is part of the bill that is presented to the President, we, as well as the President's other senior advisors, will recommend that he veto the bill.

Imposition of a "Specific Individual Target" Test (No. 3912). This amendment, which was part of the Judiciary Committee substitute, would require the Attorney General and the Director of National Intelligence to certify that any acquisition "is limited to communications to which any party is a specific individual target (which shall not be limited to known or named individuals) who is reasonably believed to be located outside the United States." This provision could hamper United States intelligence operations that currently are authorized to be conducted overseas and that could be conducted more effectively from the United States without harming the privacy interests of United States persons. For example, the intelligence community may wish to target all communications in a particular neighborhood abroad before our armed forces conduct an offensive. This amendment could prevent the intelligence community from targeting a particular group of buildings or a geographic area abroad to collect foreign intelligence prior to such military operations. This restriction could have serious consequences on our ability to collect necessary foreign intelligence information, including information vital to conducting military operations abroad and protecting the lives of our service members, and it is unacceptable. Imposing such additional requirements to the carefully crafted framework provided by S. 2248 would harm important intelligence operations without appreciably enhancing the privacy interests of Americans. If this amendment is part of the bill that is

The Honorable Harry Reid

presented to the President, we, as well as the President's other senior advisors, will recommend that he veto the bill.

Limits Dissemination of Foreign Intelligence Information (No. 3915). This amendment originally was offered in the Senate Intelligence Committee, where it was rejected on a 10-5 vote. The full Senate then rejected the amendment as part of its consideration of the Judiciary Committee amendment. The proposed amendment would impose significant new restrictions on the use of foreign intelligence information, including information not concerning United States persons, obtained or derived from acquisitions using targeting procedures that the FISA Court later found to be unsatisfactory for any reason. By requiring analysts to go back to the relevant databases and extract certain information, as well as to determine what other information is derived from that information, this requirement would place a difficult, and perhaps insurmountable, operational burden on the intelligence community in implementing authorities that target terrorists and other foreign intelligence targets located overseas. The effect of this burden would be to divert analysts and other resources from their core mission—protecting the Nation—to search for information, including information that does not concern United States persons. This requirement also stands at odds with the mandate of the September 11th Commission that the intelligence community should find and link disparate pieces of foreign intelligence information. Finally, the requirement would actually degrade—rather than enhance—privacy protections by requiring analysts to locate and examine United States person information that would otherwise not be reviewed. Accordingly, if this amendment is part of the bill that is presented to the President, we, as well as the President's other senior advisors, will recommend that he veto the bill.

II. Liability Protection for Telecommunications Companies

Several amendments to S. 2248 would alter the carefully crafted provisions in that bill that afford liability protection to those companies believed to have assisted the Government in the aftermath of the September 11th attacks. Extending liability protection to such companies is imperative; failure to do so could limit future cooperation by such companies and put critical intelligence operations at risk. Moreover, litigation against companies believed to have assisted the Government risks the disclosure of highly classified information regarding extremely sensitive intelligence sources and methods. If any of these amendments is part of the bill that is presented to the President, we, as well as the President's other senior advisors, will recommend that he veto the bill.

Striking the Immunity Provisions (No. 3907). This amendment would strike Title II of S. 2248, which affords liability protection to telecommunications companies believed to have assisted the Government following the September 11th attacks. This amendment also would strike the important provisions in the bill that would establish procedures for implementing existing statutory defenses in the future and that would preempt state investigations of assistance provided by any electronic communication service provider to an element of the intelligence community. Those provisions are important to ensuring that electronic communication service providers can take full advantage of existing immunity provisions and to protecting highly classified information.

The Honorable Harry Reid

Affording liability protection to those companies believed to have assisted the Government with communications intelligence activities in the aftermath of September 11th is a just result and is essential to ensuring that our intelligence community is able to carry out its mission. After reviewing the relevant documents, the Intelligence Committee determined that 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. In its Conference Report, the Committee "concluded that the providers . . . had a good faith basis" for responding to the requests for assistance they received. The Senate Intelligence Committee ultimately agreed to necessary immunity protections on a nearly-unanimous, bipartisan, 13-2 vote. Twelve Members of the Committee subsequently rejected a motion to strike this provision.

The immunity offered in S. 2248 applies only in a narrow set of circumstances. An action may be dismissed only if the Attorney General certifies to the court that either: (i) the electronic communications service provider did not provide the assistance; or (ii) the assistance was provided in the wake of the September 11th attacks, and was described in a written request indicating that the activity was authorized by the President and determined to be lawful. A court must review this certification before an action may be dismissed. This immunity provision does not extend to the Government or Government officials, and it does not immunize any criminal conduct.

Providing this liability protection is critical to the national security. As the Intelligence Committee recognized, "the intelligence community cannot obtain the intelligence it needs without assistance from these companies." That committee also recognized that companies in the future may be less willing to assist the Government if they face the threat of private lawsuits each time they are alleged to have provided assistance. The committee concluded that: "The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation." Allowing continued litigation also risks the disclosure of highly classified information regarding intelligence sources and methods. In addition to providing an advantage to our adversaries, the potential disclosure of classified information puts the facilities and personnel of electronic communication service providers at risk.

For these reasons, we, as well as the President's other senior advisors, will recommend that he veto any bill that does not afford liability protection to these companies.

Substituting the Government as the Defendant in Litigation (No. 3927). This amendment would substitute the United States as the party defendant for any covered civil action against a telecommunications provider if certain conditions are met. The Government would be substituted if the FISA Court determined that the company received a written request that complied with 18 U.S.C. § 2511(2)(a)(ii)(B), an existing statutory protection; the company acted in "good faith . . . pursuant to an objectively reasonable belief" that compliance with the written request was permitted by law; or that the company did not participate.

Substitution is not an acceptable alternative to immunity. Substituting the Government would simply continue the litigation at the expense of the American taxpayer. Substitution does nothing to reduce the risk of the further disclosure of highly classified information. The very point of these lawsuits is to prove plaintiffs' claims by disclosing classified information

The Honorable Harry Reid

regarding the activities alleged in the complaints, and this amendment would permit plaintiffs to participate in proceedings before the FISA Court regarding the conduct at issue. A judgment finding that a particular company is a Government partner also could result in the disclosure of highly classified information regarding intelligence sources and methods and hurt the company's reputation overseas. In addition, the companies would still face many of the burdens of litigation – including attorneys' fees and disruption to their businesses from discovery – because their conduct will be the key question in the litigation. Such litigation could deter private sector entities from providing assistance to the intelligence community in the future. Finally, the lawsuits could result in the expenditure of taxpayer resources, as the U.S. Treasury would be responsible for the payment of an adverse judgment. If this amendment is part of the bill that is presented to the President, we, as well as the President's other senior advisors, will recommend that he veto the bill.

FISA Court Involvement in Determining Immunity (No. 3919). This amendment would require all judges of the FISA Court to determine whether the written requests or directives from the Government complied with 18 U.S.C. § 2511(2)(a)(ii), an existing statutory protection; whether companies acted in “good faith reliance of the electronic communication service provider on the written request or directive under paragraph (1)(A)(ii), such that the electronic communication service provider had an objectively reasonable belief under the circumstances that the written request or directive was lawful”; or whether the companies did not participate in the alleged intelligence activities.

This amendment is not acceptable. It is for Congress, not the courts, to make the public policy decision whether to grant liability protection to telecommunications companies who are being sued simply because they are alleged to have assisted the Government in the aftermath of the September 11th attacks. The Senate Intelligence Committee has reviewed the relevant documents and concluded that those who assisted the Government acted in good faith and received written assurances that the activities were lawful and being conducted pursuant to a Presidential authorization. This amendment effectively sends a message of no-confidence to the companies who helped our Nation prevent terrorist attacks in the aftermath of the deadliest foreign attacks on U.S. soil. Transferring a policy decision critical to our national security to the FISA Court, which would be limited in its consideration to the particular matter before them (without any consideration of the impact of immunity on our national security), is unacceptable.

In contrast to S. 2248, this amendment would not allow for the expeditious dismissal of the relevant litigation. Rather, this amendment would do little more than transfer the existing litigation to the full FISA Court and would likely result in protracted litigation. The standards in the amendment also are ambiguous and would likely require fact-finding on the issue of good faith and whether the companies “had an objectively reasonable belief” that assisting the Government was lawful—even though the Senate Intelligence Committee has already studied this issue and concluded such companies did act in good faith. The companies being sued would continue to be subjected to the burdens of the litigation, and the continued litigation would increase the risk of the disclosure of highly classified information.

The procedures set forth under the amendment also present insurmountable problems. First, the amendment would permit plaintiffs to participate in the litigation before the FISA

The Honorable Harry Reid

Court. This poses a very serious risk of disclosure to plaintiffs of classified facts over which the Government has asserted the state secrets privilege and of disclosure of these secrets to the public. The FISA Court safeguards national security secrets precisely because the proceedings are generally *ex parte*—only the Government appears. The involvement of plaintiffs also is likely to prolong the litigation. Second, assembling the FISA Court for en banc hearings on these cases could cause delays in the disposition of the cases. Third, the amendment would purport to abrogate the state secrets privilege with respect to proceedings in the FISA Court. This would pose a serious risk of harm to the national security by possibly allowing plaintiffs access to highly classified information about sensitive intelligence activities, sources, and methods. The conclusion of the FISA Court also may reveal sensitive information to the public and our adversaries. Beyond these serious policy considerations, it also would raise very serious constitutional questions about the authority of Congress to abrogate the constitutionally-based privilege over national security information within the Executive's control. This is unnecessary, because classified information may be shared with a court *in camera* and *ex parte* even when the state secrets privilege is asserted. Fourth, the amendment does not explicitly provide for appeal of determinations by the FISA Court. Finally, imposing a standard involving an "objectively reasonable belief" is likely to cause companies in the future to feel compelled to make an independent finding prior to complying with a lawful Government request for assistance. Those companies do not have access to information necessary to make this judgment. Imposition of such a standard could cause dangerous delays in critical intelligence operations and put our national security at risk. As the Intelligence Committee recognized in its report on S. 2248, "the intelligence community cannot obtain the intelligence it needs without assistance from these companies." For these reasons, existing law rightly places no such obligation on telecommunications companies.

If this amendment is part of the bill that is presented to the President, we, as well as the President's other senior advisors, will recommend that he veto the bill.

III. Other Amendments

Imposing a Short Sunset on the Legislation (No. 3930). This amendment would shorten the existing sunset provision in S. 2248 from six years to four years. We strongly oppose it. S. 2248 should not have an expiration date at all. The threats we face do not come with an expiration date, and our authorities to counter those threats should be placed on a permanent foundation. They should not be in a continual state of doubt. Any sunset provision withholds from our intelligence professionals and our private partners the certainty and permanence they need to protect Americans from terrorism and other threats to the national security. The intelligence community operates much more effectively when the rules governing our intelligence professionals' ability to track our adversaries are established and are not changing from year to year. Stability of law also allows the intelligence community and our private partners to invest resources appropriately. Nor is there any need for a sunset. There has been extensive public discussion, debate, and consideration of FISA modernization and there is now a lengthy factual record on the need for this legislation. Indeed, Administration officials have been working with Congress since at least the summer of 2006 on legislation to modernize FISA. There also has been extensive congressional oversight and reporting regarding the Government's use of the authorities under the Protect America Act. In addition, S. 2248 includes substantial

The Honorable Harry Reid

congressional oversight of the Government's use of the authorities provided in the bill. This oversight includes provision of various written reports to the congressional intelligence committees, including semiannual assessments by the Attorney General and the Director of National Intelligence, assessments by each relevant agency's Inspector General, and annual reviews by the head of any agency conducting operations under Title VII. Congress can, of course, revisit these issues and amend a statute at whatever time it chooses. We therefore urge Congress to provide a long-term solution to an out-dated FISA and to resist attempts to impose a short expiration date on this legislation. Although we believe that any sunset is unwise and unnecessary, we support S. 2248 despite its six-year sunset because it meets our operational needs to keep the country safe by providing needed authorities and liability protection.

Imposes Court Review of Compliance with Minimization Procedures (No. 3920). This amendment, which was part of the Judiciary Committee substitute, would allow the FISA Court to review compliance with minimization procedures that are used on a programmatic basis for the acquisition of foreign intelligence information by targeting individuals reasonably believed to be outside the United States. We strongly oppose this amendment. It could place the FISA Court in a position where it would conduct individualized review of the intelligence community's foreign communications intelligence activities. While conferring such authority on the court is understandable in the context of traditional FISA collection, it is anomalous in this context, where the court's role is in approving generally applicable procedures for collection targeting individuals outside the United States.

Congress is aware of the substantial oversight of the use of the authorities contained in the Protect America Act. As noted above, S. 2248 significantly increases such oversight by mandating semiannual assessments by the Attorney General and the Director of National Intelligence, assessments by each relevant agency's Inspector General, and annual reviews by the head of any agency conducting operations under Title VII, as well as extensive reporting to Congress and to the FISA Court. The repeated layering of overlapping oversight requirements on one aspect of intelligence community operations is both unnecessary and not the best use of limited resources and expertise.

Expedited FISA Court Review of Challenges and Petitions to Compel Compliance (No. 3941). This amendment would require the FISA Court to make an initial ruling on the frivolousness of a challenge to a directive issued under the bill within five days, and to review any challenge that requires plenary review within 30 days. The amendment also provides that if the Constitution requires it, the court can take longer to decide the issues before it. The amendment sets forth similar procedures for the enforcement of directives (*i.e.*, when the Government seeks to compel an electronic communication service provider to furnish assistance or information). This amendment would ensure that challenges to directives and petitions to compel compliance with directives are adjudicated in a manner that avoids undue delays in critical intelligence collection. This amendment would improve the existing provisions in S. 2248 pertaining to challenges to directives and petitions to compel cooperation by electronic communication service providers, and we strongly support it.

Proliferation of Weapons of Mass Destruction (No. 3938). This amendment, which would apply to surveillance pursuant to traditional FISA Court orders, would expand the definition of

The Honorable Harry Reid

"foreign power" to include groups engaged in the international proliferation of weapons of mass destruction. This amendment reflects the threat posed by these catastrophic weapons and extends FISA to apply to individuals and groups engaged in the international proliferation of such weapons. To the extent that they are not also engaged in international terrorism, FISA currently does not cover those engaged in the international proliferation of weapons of mass destruction. The amendment would expand the definition of "agent of a foreign power" to include non-U.S. persons engaged in such activities, even if they cannot be connected to a foreign power before the surveillance is initiated. The amendment would close an existing gap in FISA's coverage with respect to surveillance conducted pursuant to traditional FISA Court orders, and we strongly support it.

Exclusive Means (No. 3910). We understand that the amendment relating to the exclusive means provision in S. 2248 is undergoing additional revision. As a result, we are withholding comment on this amendment and its text at this time. We note, however, that we support the provision currently contained in S. 2248 and to support its modification, we would have to conclude that the amendment provides for sufficient flexibility to permit the President to protect the Nation adequately in times of national emergency.

IV. Expiration

While it is essential that any FISA modernization presented to the President provide the intelligence community with the tools it needs while safeguarding the civil liberties of Americans, it is also vital that Congress not permit the authorities of the Protect America Act not be allowed simply to expire. As you are aware, the Protect America Act, which allowed us temporarily to close gaps in our intelligence collection, was to sunset on February 1, 2008. Because Congress indicated that it was "a legislative impossibility" to meet this deadline, it passed and the President signed a fifteen-day extension. Failure to pass long-term legislation during this period would degrade our ability to obtain vital foreign intelligence information, including the location, intentions, and capabilities of terrorists and other foreign intelligence targets abroad.

First, the expiration of the authorities in the Protect America Act would plunge critical intelligence programs into a state of uncertainty which could cause us to delay the gathering of, or simply miss, critical foreign intelligence information. Expiration would result in a degradation of critical tools necessary to carry out our national security mission. Without these authorities, there is significant doubt surrounding the future of aspects of our operations. For instance, expiration would create uncertainty concerning:

- The ability to modify certifications and procedures issued under the Protect America Act to reflect operational needs and the implementation of procedures to ensure that agencies are fully integrated protecting the Nation;
- The continuing validity of liability protection for those who assist us according to the procedures under the Protect America Act;
- The continuing validity of the judicial mechanism for compelling the assistance needed to protect our national security;

The Honorable Harry Reid

- The ability to cover intelligence gaps created by new communication paths or technologies. If the intelligence community uncovers such new methods, it will need to act to cover these intelligence gaps.

All of these aspects of our operations are subject to great uncertainty and delay if the authorities of the Protect America Act expire. Indeed, some critical operations will likely not be possible without the tools provided by the Protect America Act. We will be forced to pursue intelligence collection under FISA's outdated legal framework—a framework that we already know leads to intelligence gaps. This degradation of our intelligence capability will occur despite the fact that, as the Department of Justice has notified Congress, the FISA Court has approved our targeting procedures pursuant to the Protect America Act.

Second, expiration or continued short-term extensions of the Protect America Act means that an issue of paramount importance will not be addressed. This is the issue of providing liability protection for those who provided vital assistance to the Nation after September 11, 2001. Senior leaders of the intelligence community have consistently emphasized the critical need to address this issue since 2006. See, "FISA for the 21st Century" hearing before the Senate Judiciary Committee with Director of the Central Intelligence Agency and Director of the National Security Agency; 2007 Annual Threat Assessment Hearing before the Senate Select Committee on Intelligence with Director of National Intelligence. Ever since the first Administration proposal to modernize FISA in April 2007, the Administration had noted that meeting the intelligence community's operational needs had two critical components—modernizing FISA's authorities and providing liability protection. The Protect America Act updated FISA's legal framework, but it did not address the need for liability protection.

As we have discussed above, and the Senate Intelligence Committee recognized, "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." As it concluded, "[t]he possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation." In short, if the absence of retroactive liability protection leads to private partners not cooperating with foreign intelligence activities, we can expect more intelligence gaps.

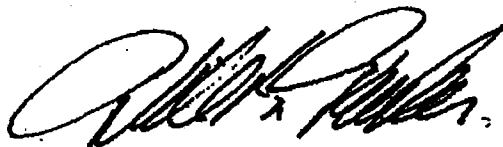
Questions surrounding the legality of the Government's request for assistance following September 11th should not be resolved in the context of suits against private parties. By granting responsible liability protection, S. 2248 "simply recognizes that, in the specific historical circumstances here, if the private sector relied on written representations that high-level Government officials had assessed the [the President's] program to be legal, they acted in good faith and should be entitled to protection from civil suit." Likewise, we do not believe that it is constructive—indeed, it is destructive—to degrade the ability of the intelligence community to protect the country by punishing our private partners who are not part of the ongoing debate between the branches over their respective powers.

The Honorable Harry Reid

The Protect America Act's authorities expire in less than two weeks. The Administration remains prepared to work with Congress towards the passage of a FISA modernization bill that would strengthen the Nation's intelligence capabilities while respecting and protecting the constitutional rights of Americans, so that the President can sign such a bill into law. Passage of S. 2248 and rejection of those amendments that would undermine it would be a critical step in this direction. We look forward to continuing to work with you and the Members of the Senate on these important issues.

Thank you for the opportunity to present our views. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to the submission of this letter.

Sincerely,



Michael B. Mukasey
Attorney General



J.M. McConnell
Director of National Intelligence

cc: The Honorable Mitch McConnell
Minority Leader
The Honorable Patrick Leahy
Chairman, Committee on the Judiciary
The Honorable Arlen Specter
Ranking Minority Member, Committee on the Judiciary
The Honorable John D. Rockefeller
Chairman, Select Committee on Intelligence
The Honorable Christopher S. Bond
Vice Chairman, Select Committee on Intelligence

Attachments



U.S. Department of Justice
Office of Legislative Affairs

Washington, D.C. 20530

January 25, 2008

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 for the record, which were posed to former Attorney General Alberto Gonzales following his appearance before the Committee on July 24, 2007. The hearing concerned Department of Justice Oversight. This submission provides responses to a large number of questions posed by the Committee. The Department is working expeditiously to provide the remaining responses, and we will forward them to the Committee as soon as possible.

The Office of Management and Budget has advised us that from the perspective of the Administration's program, they have no objection to the submission of this letter.

We hope this information is helpful. Please do not hesitate to contact this office if we may be of further assistance with this, or any other matter.

Sincerely,

Brian A. Benczkowski
Principal Deputy Assistant Attorney General

Enclosures

cc: The Honorable Arlen Specter
Ranking Minority Member

OAG-2

**Questions for the Record
Posed to former Attorney General Gonzales
Following the July 24, 2007,
Senate Committee on the Judiciary Hearing
Regarding DOJ Oversight
Part 1**

NOT RESPONSIVE

NOT RESPONSIVE

Specter 56 The Administration has produced legislation, the FISA Modernization Act of 2007, to modernize the FISA. This was first introduced near the end of the last Congress. In your testimony, you stated that “While FISA has been and continues to be one of our most valuable intelligence tools, it is imperative that the statute be modernized to account for the new technologies and threats of the 21st century. It has been almost thirty years since FISA was enacted, and revolutionary advances in telecommunications technology in that time have upset the delicate balance that the Congress originally struck in the statute. As a result, FISA now imposes a regime of court approval on a wide range of intelligence activities that do not substantially implicate the privacy interests of Americans—an unintended consequence that has impaired our intelligence capabilities. In many cases, FISA now requires the Executive Branch to obtain court orders to monitor the communications of individuals posing a threat to our national security located overseas. This process of obtaining a court order necessarily slows, and in some cases may prevent, the Government’s efforts to conduct surveillance of communications that are potentially vital to protecting the national security. This situation is unacceptable—we must quickly reform FISA’s outdated legal framework and ensure

that the Intelligence Community is able to gather the information it needs to protect the Nation.” However, in the February 6, 2006 hearing that the Senate Judiciary held on the TSP, you stated: “And I know today there’s going to be some discussion about whether or not we should amend FISA. I don’t know that FISA needs to be amended per se. Because when you think about it, FISA covers much more than international surveillance. It exists even in the peacetime. And so when you’re talking about domestic surveillance during peacetime, I think the procedures of FISA, quite frankly, are quite reasonable. And so that’s one of the dangers of trying to seek an amendment to FISA is that there are certain parts of FISA that I think provide good protections. And to make an amendment to FISA in order to allow the activities the president has authorized, I’m concerned will jeopardize this program.” However, in your letter dated January 17, 2007 to Chairman Leahy and me, you informed us: That on January 10, the FISA Court issued orders “authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization.” You further said that in light of this order, “any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court.” You also informed us that the President had determined not to reauthorize the Terrorist Surveillance Program because the FISA Court orders will “allow the necessary speed and agility.” In light of these statements, could you tell me why the Administration wishes to modernize the FISA?

ANSWER: The prior statements you cited are not inconsistent with the continuing need to modernize FISA and the existence of the FISA Court orders does not alter the need to modernize FISA permanently and comprehensively to reflect the new threats and technologies of the 21st Century. Changes in telecommunications technologies since 1978 have resulted in FISA’s requiring the Government to obtain court orders to intercept the communications of persons overseas—a result that hampers our intelligence capabilities in a manner that we believe was not intended by FISA’s drafters and that does not advance the privacy interests of Americans in the United States. It simply makes no sense to extend FISA Court procedures and protections to terrorist suspects overseas. The Administration’s FISA modernization proposal incorporates many provisions supported by members of Congress last year—including several proposals made in the bill you introduced, S. 2453 (National Security Surveillance Act of 2006).

The Protect America Act of 2007, which passed the Senate and House with bipartisan support, was a good start. We urge Congress to make that Act permanent and to enact other important reforms to FISA. In particular, it is imperative that Congress provide liability protection to companies alleged to have assisted the Government with intelligence activities in the wake of the September 11 attacks. The Department of Justice looks forward to working with the Congress, and with this Committee, on this important issue.

Specter 57 I am concerned about the provision in the Administration’s recent FISA bill that grants immunity for telecommunications companies that have cooperated with the Terrorist Surveillance Program (or any other intelligence surveillance program) since the Sept. 11, 2001, attacks. (Section 408). The White House has failed to provide

Congress with sufficient information about the role of the companies in the Terrorist Surveillance Program or any other program. Congress cannot grant these companies blanket immunity without first learning the facts. For this provision to even be considered, the Administration will have to provide a detailed briefing to Congress about the role these telecommunication companies have played. To this end, what plans have been made to brief the Congress on these essential facts?

ANSWER: Throughout the war on terror, the Administration has notified the Congress about the classified intelligence activities of the United States through appropriate briefings of the Intelligence Committees and congressional leadership. For example, the full membership of each Intelligence Committee has been briefed on the Terrorist Surveillance Program, as have other members of the congressional leadership. Under the National Security Act and the well-established and bipartisan tradition and understanding of both the Executive Branch and Congress, these are the appropriate Committees and Members to address such issues.

With respect to the details you seek, negotiations between the Chairman and the Administration continue on these matters. We are not able to provide additional details on any planned briefings at this time. Nevertheless, we think it is imperative to enact meaningful protection for those who are alleged to have assisted the Government in a time of great need.



NOT RESPONSIVE

NOT RESPONSIVE

Feingold 292 The Administration sent legislation to Congress in April that, while billed as “modernization” of the Foreign Intelligence Surveillance Act, contains provisions having nothing to do with modernization of FISA. Please answer each of the following questions individually. Why did the Administration decide to include a provision in its proposal that would grant immunity retroactively to individuals who cooperated with the government in certain unidentified intelligence activities?

ANSWER: Private industry partners alleged to have cooperated with the Government to ensure our nation is protected against another attack should not be held liable for any assistance they are

alleged to have provided. Such litigation risks the disclosure of state secrets and could seriously damage our national interests. We believe that 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.

Feingold 293 Why did the Administration decide to include a provision in its proposal that would permit the Attorney General to transfer any pending lawsuits challenging the legality of any “classified communications intelligence activity” to the secret, ex parte FISA Court?

ANSWER: The provision you reference is section 411 of the comprehensive FISA modernization proposal the Director of National Intelligence submitted to Congress in April 2007. Section 411 is designed to protect sensitive national security information and would allow for the transfer of litigation involving sensitive national security information to the FISA Court in specified circumstances. This provision would require a court to transfer a case to the FISA Court if: (1) the case is challenging the legality of a classified communications intelligence activity relating to a foreign threat, or the legality of any such activity is at issue in the case, and (2) the Attorney General files an affidavit under oath that the case should be transferred because further proceedings in the originating court would harm the national security of the United States. By providing for the transfer of such cases to the FISA Court, section 411 ensures that, if needed, judicial review may proceed before the court most familiar with communications intelligence activities and most practiced in safeguarding the type of national security information involved. Section 411 also provides that the decisions of the FISA Court in cases transferred under this provision would be subject to review by the FISA Court of Review and the Supreme Court of the United States.

Feingold 294 You state in your testimony that this FISA proposal includes provisions that “strengthen the privacy protections for U.S. persons in the United States.” Please specifically identify each of those provisions, including the section number, and explain how they strengthen privacy protections.

ANSWER: There are many sections in the comprehensive FISA modernization proposal the Director of National Intelligence submitted to Congress in April 2007, working in combination, that would enhance the privacy protections for U.S. persons in the United States. FISA Court and the Government to devote more resources to the preparation and review of applications to conduct surveillance that most directly implicate the privacy interests of persons in the United States. We urge Congress to make that Act permanent and to enact other important reforms to modernize and streamline FISA.

NOT RESPONSIVE

NOT RESPONSIVE

NOT RESPONSIVE

Feingold 308 FISA requires that the Department issue a report to the Judiciary and Intelligence Committees every six months on its implementation of FISA. By statute, it must include “a summary of significant legal interpretations of [FISA] involving matters before the Foreign Intelligence Surveillance Court,” as well as copies of all decisions and opinions of the FISA Court. When the Department submits its report covering the first half of 2007, will it comply fully with that statute?

ANSWER: The provision you reference, 50 U.S.C. § 1871, requires the Department to report semiannually, “in a manner consistent with the protection of the national security,” specified information, including “a summary of significant legal interpretations of [FISA] involving matters before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review” and “copies of all decisions (not including orders) or opinions” of those courts containing “significant construction or interpretation of the provisions” of FISA.

The Department will issue its next semiannual report at the end of the year, and that report will be consistent with these requirements.

NOT RESPONSIVE

Gerry, Brett

From: Eisenberg, John
Sent: Thursday, December 13, 2007 3:35 PM
To: Gerry, Brett
Subject: Why didn't you come?

FOIA EXEMPTION b(5)



OAG-22



U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 5, 2007

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

The Honorable John D. Rockefeller IV
Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

The Honorable John Conyers, Jr.
Chairman
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

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

Dear Messrs. Chairmen:

On August 5, 2007, the President signed the Protect America Act of 2007 ("Act"), which amended the Foreign Intelligence Surveillance Act of 1978 (FISA). The Act moves FISA toward its original focus and provides critical new authority to conduct surveillance on foreign intelligence targets located overseas with more of the speed and agility necessary to safeguard the American people. We are grateful to Congress for identifying and remedying the vulnerability caused by the outdated FISA statute.

The Department of Justice is committed to ensuring that any use of the new authority is consistent with the Act and with the protection of the privacy and civil liberties of Americans. Use of this authority will be subject to rigorous oversight by any intelligence agency that uses it, by the Department, and by the Office of the Director of National Intelligence (ODNI). In addition, the Department will inform Congress of acquisitions authorized by the Attorney General and the Director of National Intelligence and of the reviews it conducts to assess compliance by the implementing agencies.

The implementation and use of this new authority will be subject to the following oversight measures:

- Regular reviews by the internal compliance office of any agency that exercises authority given it under section 105B of FISA;

DAG-118A

- An audit/review by the Department 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;
- Subsequent audit/reviews by the Department and ODNI at least once every thirty days;
- An agency using this authority will be under an ongoing obligation to report promptly to the Department and to ODNI incidents of noncompliance by its personnel.

The Department's compliance audits/reviews will be conducted by attorneys of the Department's 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 Officer.

The Department also appreciates the need for regular and meaningful reporting to Congress, so that Congress can fully understand our use of this surveillance authority as it considers its reauthorization. Accordingly, the Department will make itself available to brief and report to the committees listed below and their staff in the following ways:

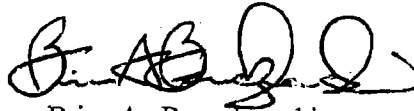
- The Act requires the Attorney General to report on acquisitions under section 105B on a semiannual basis to the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on the Judiciary of the Senate and of the House of Representatives. This report must include incidents of noncompliance with the procedures used to determine whether a person is reasonably believed to be located outside the United States, noncompliance by a recipient of a directive, and the number of certifications issued during the reporting period.
- In addition to fulfilling these statutory requirements, Department representatives will be available to brief these committees after completing the first compliance review and after each subsequent review. At these briefings, Department representatives will report on the results of the compliance review, as well as incidents of noncompliance reported to it by an implementing agency. Such briefings will also include a discussion of what remedial efforts have been or will be undertaken in light of the findings of these reviews. The Department will make available to the committees any written reports of these reviews.

The Honorable Patrick J. Leahy, John D. Rockefeller IV, John Conyers, Jr., and Silvestre Reyes
Page Three

- Department representatives will be available to brief the committees on a monthly basis to update them on the results of further compliance reviews and generally on our use of the authority under section 105B.
- 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.

The Department is committed to working with the Congress to ensure that the authority granted by the Act is used to safeguard the nation's security in a manner consistent with the privacy and civil liberty interests of Americans. Please do not hesitate to contact this office if we may be of further assistance.

Sincerely,



Brian A. Benczkowski
Principal Deputy Assistant Attorney General

cc: The Honorable Arlen Specter
The Honorable Christopher S. Bond
The Honorable Lamar S. Smith
The Honorable Peter Hoekstra

FISA Modernization White Paper

Senator Christopher S. Bond

Introduction

The need to modernize the Foreign Intelligence Surveillance Act (FISA) has affected the activities of all three branches of the United States government. The Executive branch recently identified a crucial shortfall in its ability to collect foreign intelligence against foreign targets overseas, and as a result provided the Congress with a comprehensive and well-vetted request for FISA modernization in April 2007. The judiciary has been affected, because it does not make sense to have the FISA Court spend so much time on foreign target applications involving minimal privacy interests of Americans. The Legislative branch provided a short-term solution to the intelligence gap problem by passing the "Protect America Act of 2007" in early August. However, this legislation did not include provisions that would streamline the FISA application and court order processes or grant retroactive carrier liability protection. Additionally, certain privacy measures may be incorporated to ensure clearer privacy protections for all Americans.

Given the six-month sunset on the Protect America Act, the Congress needs to act swiftly in a bipartisan manner to develop a bill containing comprehensive FISA modernization provisions. These modernization provisions must address three key areas: (1) targeting foreign persons abroad; (2) FISA streamlining; and (3) carrier liability.

Problem #1—Targeting Foreign Persons Abroad

The Intelligence Community's declining ability to target foreign persons abroad without a court order has been the primary driver behind the push for FISA modernization. It is, by far, the most complicated of the three problems and requires an understanding of the following subissues: (1) prior court approval; (2) foreign-to-foreign communications; (3) significant contacts with the United States; (4) the definition of "electronic surveillance"; (5) minimization procedures; (6) Section 2.5 of Executive Order 12333; and (7) reporting and auditing requirements. An understanding of these issues allows a more thorough assessment of the various FISA modernization proposals that have been advanced since April 2007.

Prior Court Approval

The National Security Agency has been targeting international radio communications successfully *without prior judicial authorization* since its inception in 1952. When FISA was enacted in 1978, nearly all international communications were transmitted via satellite/radio networks. The FISA definition of the term "electronic surveillance" was specifically drafted *to exclude the interception of international satellite/radio communications of persons outside the United States*. "Electronic surveillance" is a legal term of art that is often confusing because it excludes types of electronic surveillance from the technical definition, which in today's parlance are referred to as "acquisition activities." Also, FISA contains no geographical restriction on NSA's ability to conduct its foreign signals intelligence mission against radio communications networks, which means it can acquire international

0A6-182 A

radio communications anywhere in the world, **including the United States**. Thus, as enacted, FISA did not negatively impact NSA's core ability to collect international communications.

Since FISA was enacted, however, there has been a steady migration of international communications from satellite/radio networks to wire communications networks. The growth of the Internet also factored into this migration. These developments created a problem for NSA because the FISA definition of "electronic surveillance" pertaining to wire communications does not contain an exclusion for international communications and applies to the acquisition of wire communications within the United States. See 50 U.S.C. 1801(f)(2). As a result, NSA could not acquire international wire communications in the United States without first obtaining an order from the FISC. In other words, NSA could not target **international communications transmitted over wire communications networks with the same speed and flexibility that it could with respect to radio communications**.

Shortly after the al-Qa'ida terrorist attacks of September 11, 2001, the President authorized the warrantless collection of international communications against al-Qa'ida and briefed the Gang of Eight on the surveillance program. On December 16, 2005, the New York Times published a story that revealed the existence of the President's Terrorist Surveillance Program.

In January 2007, the President announced that any electronic surveillance that was occurring as part of the TSP would now be conducted subject to the approval of the FISC. In April 2007, the ODNI provided Congress with a comprehensive and well-vetted request for FISA modernization. Prior to the August recess, the Director of National Intelligence (DNI) informed the Congress that the Intelligence Community was "missing a significant amount of foreign intelligence that we should be collecting to protect our country" as a result of outdated FISA provisions. Congress responded by passing the Protect America Act of 2007, which is scheduled to sunset in early February 2008.

Some recent FISA modernization proposals contained provisions that would require prior court approval before an acquisition activity could be initiated against a foreign target overseas. The proposals varied in the scope of judicial review required by the FISC. Some of the early proposals required, among other items, a description of the methods used to determine that the target is outside of the United States (including audit procedures), a description of the nature of the information sought, and a statement of the means by which the surveillance would be effected. Although these requirements are considerably less burdensome than meeting a probable cause requirement, it is likely that the FISC might require these descriptions for each foreign collection, which would require the diversion of NSA personnel to the FISA process. Such proposals would worsen the intelligence gap problem rather than solve it. Other proposals actually required that very little information be provided to the FISC, *i.e.*, no requirement to specify a target or identify the facilities or premises subject to the acquisition activity. These provisions raise a potential vulnerability in that the FISC might determine that the resulting court order is a "general warrant," and therefore unconstitutional.

Near the end of the pre-recess FISA modernization negotiation process, the DNI submitted a counterproposal that allowed the DNI and Attorney General to immediately authorize certain acquisitions of foreign intelligence information, followed by an application within 90 days of the initiation of acquisition. This proposal also contained an additional procedure whereby the Attorney General could apply to the FISC for a court order concerning persons reasonably believed to be outside of the United States. The scope of judicial review allowed, however, required the FISC judge to approve an application, unless he determined that the certification was clearly erroneous. This raised concerns that the FISC would opine that this limited review amounted to nothing more than an advisory opinion

and, therefore, the court would decline to authorize the acquisition activity. The DNI's court approval provision also required no specificity as to facilities.

Post-court review of an acquisition program is less problematic than prior court approval. The initial activity is authorized by statute, so the judicial review does not significantly affect either the legality or operation of the underlying intelligence activity. Again, the scope of judicial review is important here. If the requirements are too burdensome, it will likely have a negative impact on the NSA's operational effectiveness. Conversely, if the scope of review is too narrow, it is likely the FISC would decline to issue an advisory opinion on the legality of the given acquisition activity. The Protect America Act contains a post-court review procedure that allows the FISC to review, under a clearly erroneous standard, the government's determination that the acquisition procedures are reasonably designed to ensure that the acquisitions do not meet the FISA definition of "electronic surveillance."

Foreign-to-Foreign Communications

A number of proposals purported to solve the problem of targeting foreign persons abroad by including a provision that no court order is required for the electronic surveillance of any communications between persons that are not located within the United States, regardless of whether the communication passes through the United States or the surveillance device is located within the United States. Exclusion of foreign-to-foreign communications does not equate to an ability to target foreign persons abroad. The Intelligence Community has been quite clear on this point. NSA lawyers have informed the Congress that there are two main problems with a grant to collect only foreign-to-foreign communications. It is not always possible to identify in advance whom a foreign target will contact and this operational reality makes the so-called "foreign-to-foreign" solution of little use to the Intelligence Community. The "foreign-to-foreign" approach just does not solve the problem, because this uncertainty would still require the Intelligence Community to obtain a court order for foreign targets.

The DNI has presented two possible solutions for the foreign targeting problem that do not involve prior court approval. The first approach, which will be discussed in greater detail below, is to adopt a technology neutral definition of the FISA term "electronic surveillance." This approach has the advantage of returning FISA to its original state by excluding the targeting of any type of communication by persons abroad from the scope of the FISA process. The second approach reaches the same result by a different path, and was adopted by Congress in the Protect America Act. It clarified that nothing in the FISA definition of "electronic surveillance" should be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States. Again, this approach excludes targeting of persons abroad from the "electronic surveillance" definition and permits the upfront collection of any form of communications technology. Both of these solutions rely upon ***after-the-fact minimization procedures*** to protect the privacy interests of persons in the United States, just as NSA has been doing with respect to radio communications since its inception.

Significant Contacts

A related issue raised in some FISA modernization proposals was a requirement that the government establish guidelines to ensure that FISA electronic surveillance ***orders are sought on foreign targets outside of the United States*** when there is reason to believe ***that a significant number of communications*** to or from that person involve a person who is in the United States. ***For operational and legal reasons, the DNI objected to any proposal containing this requirement.*** As will be explained in greater detail, *infra*, the minimization procedures in use against these foreign targets provide more

than adequate protection for any persons in the United States whose communications are incidentally collected. Moreover, if those persons in the United States become of investigative interest, then standard operating procedure would lead the Intelligence Community to seek a FISC electronic surveillance order on such persons in the United States.

Electronic Surveillance

Since some of the modernization proposals either modify or clarify the FISA definition of the term "electronic surveillance," it is provided below in its entirety. It is a complicated definition that contains four parts. These parts operate together to exclude the targeting of radio communications by persons abroad from the scope of the FISA process. According to FISA, "electronic surveillance" means—

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or ***radio communications*** sent by or intended to be received by a ***particular, known United States person who is in the United States***, if the contents are acquired by ***intentionally targeting*** that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any ***wire communication*** to or from a person in the United States, without the consent of any party thereto, ***if such acquisition occurs in the United States***, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18, United States Code;

(3) the ***intentional acquisition*** by an electronic, mechanical, or other surveillance device of the contents of any ***radio communication***, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, ***and if both the sender and all intended recipients are located within the United States***; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. 1801(f) (emphasis added).

A careful reading of the statute reveals four observations about the definition that are relevant to this topic. First, the definition does not include the intentional acquisition of radio communications of persons (***either U.S. or foreign***) ***located outside of the United States*** (both the sender and all intended recipients must be located within the United States). Second, ***the definition does not preclude the collection of incidental radio communications of persons in the United States*** (particular, known United States person who is in the United States). Third, ***reverse targeting of persons within the United States falls within the definition of electronic surveillance and is thus prohibited*** (contents are acquired by intentionally targeting that United States person). Fourth, unlike the "wire communications" and "other surveillance device" components of the definition, the "radio communications" definition does not contain any geographical restrictions. See 50 U.S.C. 1801(f)(2) & (4).

The legislative history of FISA supports these observations. *First, FISA “does not afford protections to U.S. persons who are abroad, nor does it regulate the acquisition of the contents of international communications of U.S. persons who are in the United States, where the contents are acquired unintentionally.”* H. Rpt. No. 95-1283, Part II (June 8, 1978), p. 51. Second, the electronic surveillance definition does not “apply to the acquisition of the contents of international or foreign communications, where the contents are not acquired by intentionally targeting a particular known U.S. person who is in the United States.” *Id.* at 50-51. Also, “intelligence collection may be targeted against foreign or international communications but accidentally and unintentionally acquire the contents of communications intended to be totally domestic.” *Id.* at 52. Third, “only ‘intentional’ acquisitions of private domestic radio communications are within this definition because, by their very nature, radio transmissions may be intercepted anywhere in the world, even though the sender and all intended recipients are in the United States.” *Id.* Fourth, the “territorial limits of this subdefinition [50 U.S.C. 1801(f)(3)] are not dependent on the point of acquisition, as in the case of subdefinition (2), but on the locations of the sender and intended recipients of the communication.” *Id.*

As mentioned previously, the DNI has proposed a technology neutral replacement for the definition of electronic surveillance. This would help clear up the “term of art” confusion mentioned earlier. Since it does not need to make distinctions between technologies, it only has the following two parts:

(1) the installation or use of an electronic, mechanical, or other surveillance device for acquiring information by intentionally directing surveillance at **a particular, known person who is reasonably believed to be located within the United States** under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or

(2) the **intentional acquisition** of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if **both the sender and all intended recipients are reasonably believed to be located within the United States.**

A review of this definition reveals the following four observations. First, the definition does not include the intentional acquisition of communications of persons (either U.S. or foreign) located outside of the United States (both the sender and all intended recipients are reasonably believed to be located within the United States). Second, **the definition does not preclude the collection of incidental communications of persons in the United States** (particular, known United States person who is reasonably believed to be located within the United States). **To do so would make electronic collection a near impossibility.** Third, this definition has the additional advantage of **preventing the reverse targeting of person within the United States**, because such conduct would fall within the definition of electronic surveillance (by intentionally directing surveillance at a particular, known person who is reasonably believed to be located in the United States). Fourth, there are no geographical restrictions in the definition that would prevent the interception of international communications within the United States.

Minimization Procedures

The FISA definition of the term “minimization procedures” is also complicated and contains four parts, only three of which are relevant to this discussion of FISA modernization. It is important to understand the effect of these minimization procedures, because they perform a key channeling

function in the FISA process and provide significant protections for any U.S. persons whose communications have been incidentally intercepted during an acquisition activity. Instead of providing the verbatim text of the definition, it might be more useful to generally describe what is required by the three relevant parts of the minimization procedures definition.

First, the Attorney General is required to adopt specific procedures, with respect to a FISA acquisition activity or electronic surveillance, that **limit the information that can be collected, retained or disseminated concerning U.S. persons consistent with the need of the Intelligence Community** to obtain, produce, and disseminate foreign intelligence information. This is the crux of the definition and provides the general framework for protecting U.S. person information.

Second, if a FISA acquisition activity or electronic surveillance collects information about a U.S. person that is foreign intelligence information involving the national defense, the security of the United States, or the conduct of foreign affairs, **the procedures must prohibit the dissemination of such person's identity**, unless it is necessary to understand foreign intelligence information or assess its importance. Often, this type of foreign intelligence information can be disseminated without the identity of a U.S. person and still be useful to the Intelligence Community. The rule provides exceptions in only two situations, when it is necessary to understand the intelligence or to assess its importance.

Third, the minimization procedures must also provide a mechanism that **allows the retention and dissemination of evidence of a crime** that is not foreign intelligence information. For example, if an electronic surveillance reveals evidence of spousal abuse against a target suspected of being a terrorist, such evidence must be retained and disseminated appropriately even though the evidence does not fall within the definition of foreign intelligence information.

The Attorney General has developed long-standing standard minimization procedures for the FBI, NSA, and CIA that apply to the surveillances conducted by those agencies. In addition, the government may request, or the FISC might require, specialized minimization procedures that are tailored to a particular surveillance. For example, it might be necessary to set up specialized minimization procedures for the surveillance of a particular phone booth in a domestic surveillance.

The most relevant minimization procedures that affect the targeting of foreign persons abroad can be found in **United States Signals Intelligence Directive (USSID) 18**, which has been in effect since at least 1980. These detailed procedures provide **significant protections for persons in the United States whose communications are collected incidentally** during the course of an NSA acquisition activity. Except in emergency situations, these guidelines do not permit the targeting of U.S. persons abroad unless the surveillance is approved by the Attorney General. Thus, the minimization procedures incorporate the long-standing requirement of Section 2.5 of Executive Order 12333, which is discussed in greater detail in the next section.

Section 2.5 of Executive Order 12333

During the Congressional debates on the Protect America Act, concerns were raised that the Act could be used to target U.S. citizens abroad. These concerns focused on the following provisions in the Act: (1) the language clarifying that the FISA definition of "electronic surveillance" does not "encompass surveillance directed at **a person** reasonably believed to be located outside of the United States." 50 U.S.C. 1805a (emphasis added); and (2). The Act also permits the DNI and the Attorney General to "authorize the acquisition of foreign intelligence information concerning **persons** reasonably believed to be outside the United States" 50 U.S.C. 1805b(a) (emphasis added). When read in isolation, these

sections *seem to permit the targeting of U.S. citizens* reasonably believed to be outside of the United States. *However, these provisions need to be read in conjunction with the USSID 18 standard minimization procedures*, which provide significant protections for persons within the United States, and only allow for the targeting of U.S. persons abroad consistent with the requirements of Section 2.5 of Executive Order 12333 (United States Intelligence Activities). That section provides:

Attorney General Approval. The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or **against a United States person abroad**, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is **probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power**. Electronic surveillance, as defined in the Foreign Intelligence Surveillance Act of 1978, shall be conducted in accordance with that Act, as well as this Order.

Executive Order 12333, Section 2.5 (emphasis added).

The goal of the Protect America Act was to allow the Intelligence Community to collect **foreign** intelligence information on **foreign** targets located in **foreign** countries. As mentioned previously in the Foreign-to-Foreign discussion, *supra*, these provisions had to be written broadly to include "a person" or "persons" to permit the collection in the first instance. There was never any intent to allow the provision to be used to target U.S. persons abroad, and **the protections of the minimization procedures ensure such intent**.

To alleviate any concern that FISA modernization is being used as a vehicle to conduct unauthorized electronic surveillance of U.S. persons abroad, **it might make sense to incorporate the relevant text of Section 2.5 into any FISA modernization legislation**. Some might argue that the FISC should authorize such surveillance; however, U.S. courts simply do not have jurisdiction to authorize electronic surveillance in foreign countries. Any order they might issue would be a dead letter outside the United States. *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274 (1990). **Thus, it makes sense to keep the approval level with the Attorney General, the DNI, or perhaps both**. Since this provision concerns authorization for the acquisition of foreign intelligence information, the most logical place to put Section 2.5 authority would be somewhere near Section 102. Depending upon the structure of the final FISA modernization solution, the provision could be labeled as Section 102A and read as follows:

(b) Notwithstanding any other law, the Attorney General may authorize the acquisition of foreign intelligence information against a United States person reasonably believed to be outside the United States, provided that the Attorney General has determined in each case that there is probable cause to believe that the target of the acquisition activity is an agent of a foreign power under section 101(b)(2), a significant purpose of the acquisition activity is to obtain foreign intelligence information, and the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).

Congress should also consider whether the use of this authority should be included in the FISA semi-annual report.

Reporting and Auditing Requirements

A number of the FISA modernization proposals contained reporting requirements and some contained additional auditing requirements. Certainly, oversight of these important modifications to FISA is necessary, however, care should be taken to ensure that such requirements strike the right balance between obtaining useful information and not imposing too great an administrative burden on the relevant agencies. The audit provisions pose similar considerations, because ongoing audits require agency personnel to take time from their operational activities to collect information and respond to Inspector General inquiries.

Problem #2—FISA Streamlining

On July 22, 2005, the Senate Select Committee on Intelligence (SSCI) released a staff audit of the FISA process. The audit recommended that the contents of FISA applications and court orders for electronic surveillance and physical searches should be modernized and simplified.

The ODNI's April 2007 FISA modernization proposal contained three sections devoted to FISA streamlining. In general, these proposed changes would make the following changes to the application and order requirements for both electronic surveillance and physical search: (1) delete certain requirements in the applications and court orders that have proven to be unnecessary over time; (2) modify requirements to allow for less detailed description of certain items; (3) allow the President to appoint non-Senate confirmed officials to serve as certifying officials; (4) eliminate unnecessary distinctions between foreign power and agent of foreign power applications and orders; and (5) include the Director of the CIA in the list of officials who can request the Attorney General to personally review a pending FISA application.

On July 20, 2007, the FISC legal advisors provided input on the streamlining provisions contained in the ODNI's FISA modernization proposal. In general, the legal advisors were supportive of a number of the ODNI's requested changes. They also provided valuable insight about the utility of certain provisions.

Ultimately, there is likely to be bipartisan support for most of these changes. Some of the requests will need to be modified to include the input of the FISC legal advisors, and it is likely that a few requests will not be included in the FISA modernization legislation.

While many of these modifications appear to be relatively minor, they will have a positive impact on the workload of the FISC and the Department of Justice's National Security Division.

Problem #3—Carrier Liability

The issue of retrospective carrier liability must be addressed. There is nearly unanimous agreement that the telecommunications carriers alleged to have cooperated with the President's program, if they did so, should receive retroactive liability protection. The Chairman and Vice Chairman of the SSCI have both recognized that full immunity would be necessary not only to protect the companies that may have, allegedly, cooperated in good faith, but to ensure our nation's secrets

regarding methods of surveillance remain classified and are not disclosed in public through civil court cases. Substitution of the United States in place of the alleged carrier defendants will not provide adequate assurances that such secrets will remain classified. Indeed one Federal District Court has already declined to accept the government's state secrets assertion and is allowing limited discovery to proceed. I hope that a full immunity carrier liability provision will be included in the SSCI Chairman/Vice Chairman mark of a bipartisan FISA modernization proposal.