



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

November 20, 2007

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

Dear Mr. Chairman:

Enclosed please find the corrected transcript of the testimony of Mr. Kenneth Wainstein, Assistant Attorney General, National Security Division, for the hearing held before the Committee on October 31, 2007, entitled, "FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability."

If we may be of further assistance, please feel free to contact this office.

Sincerely,

For Brian A. Benczkowski
Principal Deputy Assistant Attorney General

Enclosure

OLA-19

1274207
MH

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 LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WELER, 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
ARTHUR DAVIS, Alabama
DERNIE WASSERMAN SCHULTZ, Florida
KEITH ELISON, Minnesota

LAMAR S. SMITH, Texas
RANKING MINORITY MEMBER

F. JAMES BENSENBRENNER, JR., Wisconsin
HOWARD COLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DAMEL E. LUNGREN, California
CHRIS CANNON, Utah
RIG KELLER, Florida
DARRELL E. ISSA, California
MIKE PEACE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
YRENY FRANKS, Arizona
LOUIE GOMMERT, 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>

October 9, 2007

Honorable Ken Wainstein
Assistant Attorney General for National Security
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530


Dear Mr. Wainstein:

Thank you for your recent appearance before the House Committee on the Judiciary. Your testimony on FISA and the Protect America Act was insightful and will assist the Committee in its consideration of this issue as we seek to fashion enhanced legislation.

Enclosed you will find additional questions from members of the Committee to supplement the information already provided at the September 18, 2007, hearing. As you will discover in the questions, there are some sets of questions that are specifically addressed to either you or Director Michael McConnell, while other questions request answers from both you and Director McConnell. You may choose whether to provide joint or separate answers to these latter questions. In addition, to the extent some questions (such as those initially contained in the September 11th letter to White House Counsel Fred Fielding) call for classified information, we are willing to make arrangements to receive the information in a manner that will protect its confidentiality.

Please deliver your written responses to the attention of Renata Strause of the House Committee on the Judiciary, 2138 Rayburn House Office Building, Washington, DC, 20515 no later than October 19, 2007. We would be pleased to accept answers on a 'rolling' basis in order to expedite the process. If you have any further questions or concerns, please contact Ms. Strause at (202) 225-3951.

Sincerely,



John Conyers, Jr.
Chairman

cc: Hon. Lamar S. Smith

OLA-24

**QUESTIONS FOR KEN WAINSTEIN AND MICHAEL McCONNELL
APPEARANCE BEFORE THE HOUSE JUDICIARY COMMITTEE**

September 18, 2007
2141 Rayburn House Office Building
11:00 a.m.

Questions from September 11, 2007 Letter to White House Counsel Fred Fielding
(Wainstein and McConnell)

1. The Committee sent a September 11, 2007 letter to White House Counsel Fred Fielding containing a list of questions concerning Administration foreign intelligence surveillance activities, which can be found on pages 4-5 of the attached letter. To date, we have yet to receive answers to these questions, which the White House has indicated should come from the relevant agencies. Please respond to those questions as soon as possible.

The Role of the FISA Court (FISC) (Wainstein and McConnell)

2. Under the PAA, the FISA Court only has the ability to determine whether the government is following its own procedures, and can stop the procedures only if they are "clearly erroneous." How can meaningful oversight occur if the court can only review procedures that it did not even initially approve under a "clearly erroneous" standard, rather than the underlying legality of the government's surveillance operations? Please explain.
3. The Fourth Amendment requires that the government get a warrant before invading a person's privacy. Explain how the PAA's procedures can be constitutional without any court review whatsoever, other than minimization?

Minimization (Wainstein and McConnell)

4. Is it correct that the "minimization" procedures that are to apply to surveillance under PAA are those specified under 50 U.S.C. sec. 1801(b)(1)-(3)? If not, which procedures apply?
5. There is much more strict minimization under section 4 of section 1801(h). That section applies to pre-PAA FISA surveillance that is undertaken without a warrant and without judicial pre-approval. Under those circumstances, minimization is very strict: no contents of an innocent American's communication can be disclosed, disseminated, used, or even kept for longer than 72 hours without a FISA court determination or an AG determination that the information indicates a threat of death or serious bodily harm. If there is to be any warrantless surveillance spying on Americans' conversations, wouldn't it be more prudent to subject it to the strict minimization procedures of 1801(h)(4), which already

apply to other surveillance without a court order, and not the more lax minimization that has previously applied only when a court did provide a court order before Americans were spied on? If not, why not.

6. Minimization procedures have been keep secret for the last 30 years. There are serious concerns as to how we can be assured that minimization procedures are effective for protecting Americans' privacy if we cannot see them. Would you support making minimization procedures public?
 - a) If not, why not?
 - b) Would you support producing a redacted copy?
 - c) Minimization procedures only tell you what to do with US information after it is collected, therefore not revealing sources or methods. Thus, if do not support publicizing the procedures, on what do you base your objection?
7. Would you support legislation that would sequester communications to which an American is a party (and captured under this new program) that can only be used after an application to the FISA court? If not, why not?

Scope of PAA Section 105(B) (Wainstein and McConnell)

8. Does Section 105(B) permit the President to compel communications carriers to conduct domestic wiretaps so long as "a significant purpose" is to obtain foreign intelligence information concerning persons outside the United States?
9. If an individual in the United States is suspected of working in collusion with persons outside the United States -- such that an investigation of one is in effect the investigation of the other -- under what circumstances, generally, would you use criminal or other FISA wiretaps, and under what circumstances would you use 105(B) authority? Please explain.
10. Assuming for a moment that a member of Congress is going to meet with a high-ranking official from Syria, does Section 105(B) permit the wiretapping of that Member's office phone on the grounds that it would produce "foreign intelligence information ... concerning persons reasonably believed to be outside the United States?" Please explain.
11. Does Section 105(B) permit searching stored emails of a Member of Congress who is planning to meet with Iraqi officials? Please explain.

12. Assuming for a moment that an official at a West Coast computer company is negotiating with China to sell certain computer technology -- that may or may not be sensitive, the facts are simply not certain -- does Section 105(B) permit the searching of the executive's emails on the grounds that all information associated with this transaction is "foreign intelligence information ... concerning persons reasonably believed to be outside the United States"? Please explain.
13. Under Section 105(B) does the term "acquire" include "intercept"? Can the Administration "acquire" foreign relations information concerning persons overseas by "intercepting" phone conversations in the United States? Please explain.
14. Under Section 105(B) does the term "custodian" refer to anyone other than "custodians" of communications carriers?
 - a) Can the President direct a "custodian" of a medical office to turn over medical records, if a "primary purpose" of the investigation is to obtain foreign intelligence information concerning someone who is overseas? Please explain.
 - b) Can the President direct a "custodian" of a business, bank, or credit agency to turn over financial records to the Government, so long as a "significant purpose" of the request is to obtain foreign intelligence information? Please explain.
15. Suppose an American critic of the Iraq War travels overseas, and is thus no longer in the United States. Under Section 105(B), can the President direct "custodians" of records concerning this individual, including stored electronic communications, to produce such records to the Government with no other showing of cause that is subject to judicial review? Please explain.

Telecommunications Carriers Immunity Questions (Wainstein and McConnell)

16. 18 U.S.C. § 2511(2)(a)(ii) currently provides for telecommunications carrier immunity if one of two conditions is satisfied: a) the carrier has a court order signed by an authorizing judge; or b) the carrier has a certification from the Attorney General or another statutorily authorized official that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provisions of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. Doesn't this current statutory scheme offer the necessary protection for the telecommunications industry, advance national security interests, and provide essential oversight? If not, why not?

17. Section 2511(2)(a)(ii) certification has defined preconditions that must be satisfied, including: all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provisions of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. Blanket immunity would not have the same preconditions. Given that distinction, how can we ensure that critical checks and balances exist in the surveillance framework if blanket immunity is provided?
18. If we were to give the telecommunications carriers complete, blanket immunity, how would we guard against a total disregard of the law by companies who believe that the government simply will bail them out if they overstep legal boundaries in intercepting communications?
19. If the so-called Terrorist Surveillance Program (TSP) was perfectly legal as has been claimed, why would companies who cooperated in it need immunity?
20. The pending cases against telecommunication companies are years away from final judgment. In light of that, would it be appropriate to have the discussion of retroactive immunity wait until we determine what actions actually occurred? If not, why not?
21. Would you support something more specific than the complete amnesty you propose in your draft legislation, like simply putting a damages cap on the claims? If not, why not?
22. In discussing the controversy over the PAA with the El Paso Times, DNI McConnell said "reverse targeting" was illegal, a violation of the Fourth Amendment, and that someone engaging in such offenses "could go to jail for that sort of thing." But wouldn't the immunity provisions recommended by the administration ensure that no one would go to jail for violations of the laws governing electronic surveillance for intelligence purposes?

Scope of Authority under the PAA (Wainstein and McConnell)

23. Section 105(A) exempts surveillance "directed at" people overseas from the definition of electronic surveillance, and therefore traditional FISA court review. Because surveillance only need be "directed" at people overseas, can the government under the PAA pick up all international communications into or out of the U.S., as long as one party to the call is overseas?
24. FISA has always placed the telecommunication carriers between the government and American's private communications and records. The carriers can only turn over information in response to a specific request. Now that the government has direct access to all communication streams, how can we protect against potential abuses?
25. The Administration claims that it needs heightened access to communications because it

cannot instantaneously determine the location of each party.

- a) Phone companies are capable of determining international calls versus domestic calls, and charge more for the international calls. Would it be possible for the NSA to use similar technology? If not, why not?
- b) If it cannot be determined where either end of a call is, how can purely domestic to domestic communications be isolated?
- c) Is it possible to institute a program by which there is initial collection of calls, none of the content is accessed until the locations of the parties are determined, and then it can be retained and only the foreign to foreign calls used?

Metadata Collection (Wainstein and McConnell)

26. On May 11, 2006, USA Today reported that "[t]he NSA has been secretly collecting the phone call records of tens of millions of Americans" and that "[i]t's the largest database ever assembled in the world." (See Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today, May 11, 2006). At any time from September 11, 2001 to the present, has the Administration, pursuant to foreign intelligence purposes, obtained call or e-mail record information or other external data on phone calls or e-mails made in the United States, through the gathering of "metadata" or otherwise, regardless of the specific title of the intelligence program or the agencies that conducted the program? Please explain.

FISA Exclusivity (Wainstein only)

27. Does the United States, through its Justice Department, agree that FISA is the law of the land, and that foreign intelligence surveillance must occur within that law? If not, why not?
28. Is the President free to disregard any provisions of FISA with which he disagrees? If so, please explain.
29. To your knowledge, since January of 2007, when the Attorney General stated that the TSP was brought within FISA, has all foreign intelligence electronic surveillance occurred consistent with FISA – both prior to and subsequent to the August amendments? Since that time have any electronic surveillance programs been conducted outside the authority of the Foreign Intelligence Surveillance Act as amended by the Protect America Act?

30. Does the Department of Justice still take the position that the Authorization for Use of Military Force (AUMF) related to the invasion of Iraq presently constitutes a basis for the President to disregard FISA? If so, please explain.
31. On December 22, 2005, the Department of Justice, in a letter to Congress, set forth the position that the President's inherent Article II powers permitted it to conduct certain terrorist surveillance outside of FISA. Is this still the Department of Justice's position?

The Federal Bureau of Investigation (Wainstein only)

32. DNI McConnell said the intelligence community is not doing massive data mining. But the FBI retains information from NSLs even where the information demonstrates the subject of the NSL was innocent. Why is this data being retained if not for data mining?
33. The Department of Justice Inspector General recently released an audit report regarding the Terrorist Screening Center, which revealed the Terrorist Screening Center watchlist had grown to over 724,000 records by April of 2007, and was increasing at a rate of 20,000 records per month. The IG found several known or suspected terrorists that were not watchlisted correctly, and a sample of records subjected to post-encounter quality assurance reviews showed 38 percent contained errors or inconsistencies. How can the intelligence community properly identify and target terrorists for electronic surveillance with such an incomplete terrorist watchlist?

Mismanagement in the Intelligence Community -- National Security Agency (McConnell only)

34. As the FISA Modernization Bill and the PAA were being debated in Congress, DNI McConnell and others in the administration suggested that advances in technology had created an "intelligence gap" which was making it more difficult for the intelligence community to keep America safe from terrorists. But according to a May 6, 2007 article in the Baltimore Sun, an internal NSA task force cited management problems as the cause of program upgrade delays, technology breakdowns and cost overruns, and called for a "fundamental change" in the way the NSA was managed. The report said NSA leadership "lacks vision and is unable to set objectives and meet them," and that NSA employees "do not trust our peers to deliver." These conclusions "are strikingly similar" to the conclusions of NSA management studies performed in 1999; yet even after 9/11 the fundamental changes recommended have not been made. Portions of this NSA task force report are not classified. Will you agree to release the unclassified portions of this report publicly and to the Committee?
35. Ensuring the proper management of intelligence would seem to be in many respects as important as increasing the authority to collect intelligence because, as the Joint

Intelligence Committee investigation into the 9/11 terrorist attacks showed, the NSA had intercepted communications linking the hijackers to terrorism long before 9/11 but that those intercepts, along with other critical pieces intelligence, were lost among the "vast streams" of data being collected. If we can assume that the NSA is collecting even more intelligence now than before 9/11, how can we be assured that the management problems at NSA are not hampering the intelligence community's ability to identify and understand which bits of intelligence are important and which are not? Please explain.

36. The September 14th Baltimore Sun report regarding a fire at an NSA "operations building" raises even more fundamental concerns about the NSA's ability to properly manage its operations. On August 6, 2007, right after the PAA was enacted, MSNBC and Newsweek reported that, "The National Security Agency is falling so far behind in upgrading its infrastructure to cope with the digital age that the agency has had problems with its electricity supply, forcing some offices to temporarily shut down." Please explain what steps are being taken in response to the reported fire and shutdown and other infrastructure and management problems.

German plot (McConnell only)

37. On September 10, you testified publicly before the Senate Homeland Security Committee that the temporary FISA changes due to the Protect America Act helped lead to the recent arrests of three Islamic militants accused of planning bomb attacks in Germany. But two days later, on September 12, you issued a contradictory statement, saying that "information contributing to the recent arrests was not collected under authorities provided by the Protect America Act." It has been publicly suggested that it was the pre-PAA FISA law, which you have criticized, that was used to help capture the terrorist plotters in Germany, and not the temporary Protect America Act.

- a) Was your statement on September 10, claiming that the temporary Protect America Act helped lead to the German arrests, actually false?
- b) Can you explain to us how it was that you came to give false information to the Senate Committee concerning the alleged contribution of the temporary Protect America Act to the German arrests?
- c) Is it true that it was the pre-PAA FISA law that was used to help capture the terrorist plotters in Germany, and not the temporary Protect America Act?

US persons "targeted" for surveillance (McConnell only)

38. In your recent interview with the El Paso Times, responding to a concern about "reverse

targeting," you stated that there are "100 or less" instances where a U.S. person has been targeted for surveillance.

- a) Please explain how, when, why, and by whom it was decided to declassify that information and reveal it publicly.
- b) Over how long a period of time does that "100 or less" figure apply? For example, was it one year, five years, or since 9/11?

Declassification of Information (McConnell only)

39. At the hearing, you told Representative Scott that there is a process to declassify information and that ultimately it is the responsibility for the President to decide. Later in the hearing, you told Representative Sutton that when you did an interview you could declassify information because "it was a judgment call on your part." Could you please explain the discrepancy between your two responses to similar questions?

Concerns About the House Bill (McConnell only)

40. During the hearing, in response to my question regarding the alleged 180 degree reversal of your position on the House bill regarding FISA this summer, you claimed that you had not changed your position but that once you had actually "reviewed the words" of the House bill, you could not accept it. Please explain specifically what problems you had with the "words" of the House bill.

Previous Problems Concerning Warrantless Surveillance and Minimization
(McConnell only)

41. In August 2005, the New York Times reported that John Bolton, then an official at the State Department, received summaries of intercepts that included conversations of "U.S. persons" and requested that the National Security Agency inform him who those persons were. Newsweek thereafter reported that from January 2004 to May 2005, the NSA had supplied the names of some 10,000 American citizens in this informal fashion to policy makers at many departments and law enforcement agencies. The former General Counsel at the NSA, Stewart Baker, was quoted as stating that the NSA would "typically ask why" disclosure was necessary, but "wouldn't try to second guess" the rationale.
- a) What procedures are in place by entities such as the NSA that obtain summaries of conversations intercepted without a warrant to review the requests by other agencies, such as law enforcement agencies, to disclose

the identity of "U.S. persons" whose conversations are so intercepted without a warrant?

- 1) What showing, if any, is the requesting individual/agency required to make in order to obtain the identity of the U.S. person whose conversation was intercepted?
 - 2) Are any such requests denied, and, if so, in the past five years, state how many such requests have been denied?
- b) In the past five years, how many times have the summaries of such intercepted conversations been requested by and provided to the Office of the Vice President? To the Office of the President?
 - c) In the past five years, how many times have phone conversations of federally elected officials or their staff been intercepted under any surveillance program without a warrant? Do copies of those conversations still exist?
 - d) In the past five years, how many times have phone conversations of known members of the U.S. news media been intercepted without a warrant? Do copies of those conversations still exist?
 - e) In the past five years, how many times have phone conversations of attorneys in the United States been intercepted without a warrant? Do copies of those conversations still exist?
42. In 2006, Newsweek reported that the "NSA received—and fulfilled— between 3000 and 3,500 requests from other agencies to supply the names of U.S. citizens and officials ... that initially were deleted from raw intercept reports. . . . About one third of such disclosures were made to officials at the policymaking level." (See Mark Hosenball, "Spying, Giving Out U.S. Names," Newsweek, May 2, 2006).
- a) During the operation of the "terrorist surveillance program," prior to its disclosure in the New York Times in December 2005, how many "U.S. names" that were masked from transcripts of intercepts were disclosed (unmasked) to government entities that requested the identities?
 - b) What justification was required by a requestor to obtain the identity of the U.S. person on a minimized conversation?
 - c) What criteria, if any, were used to determine whether a request for the identity of a U.S. person on a minimized interception was appropriate or

whether the identity of the U.S. person was necessary for a legitimate intelligence or law enforcement purpose?

- d) If no justifications for identity information were required, and no criteria for review to determine the appropriateness of the request were in existence, then what purpose is served by the minimization procedures that mask a U.S. person's identity as a speaker on an intercepted phone call?
 - e) By name or position, which "policy makers" requested and received identity information of U.S. persons whose communications were intercepted?
43. The TSP was described in a Department of Justice (DOJ) "white paper" as "targeting the international communications into and out of the United States of persons reasonably believed to be linked to al Qaeda" From the date of the inception of any warrantless interception program (approximately October 2001) through the 2007 decision to bring any such program under scrutiny of FISA, was the program ever broader to encompass any other international communications in addition to those reasonably believed to be linked to al Qaeda?
44. How many U.S. persons have been arrested or detained as a result of warrantless interceptions under the surveillance programs established by the President?
45. What is the date of the first document that purports to justify the warrantless surveillance program on the AUMF? How would you respond to claims that the AUMF rationale was a creation of Administration lawyers after the December 2005 New York Times article?
46. At any time from September 11, 2001 through December 2005, did the NSA obtain "trap and trace" or "pen register" information on the phones or telecommunications equipment of U.S. persons without court orders?
- a) If so, how many times?
 - b) If so, on what legal authority?
47. Since September 11, 2001, has law enforcement or the intelligence community conducted physical searches of the homes or businesses of U.S. citizens without warrants based on authorizations or approvals by the President or pursuant to a Presidentially authorized program?
48. Under the non-FISA warrantless interception programs, has law enforcement or the intelligence community deliberately caused the interception of purely domestic to domestic phone conversations without a FISA warrant? If so, what has been done with information so obtained?

49. Questions have been raised as to whether Christine Amanpour of CNN has ever had her telephone conversations intercepted by Administration surveillance programs. (See David Ensor, *NSA: Amanpour, Other CNN Reporters Not Targeted for Surveillance*, CNN, January 6, 2006). Has Ms. Amanpour ever been the target of warrantless surveillance – whether or not she was in the United States? Have any telephone conversations of Christine Amanpour been intercepted pursuant to any warrantless surveillance program?

Questions for Director McConnell
Submitted by Congressman Bob Goodlatte (VA-06)
Hearing on "Warrantless Surveillance and the Foreign Intelligence
Surveillance Act: The Role of Checks and Balances in Protecting Americans'
Privacy Rights (Part II)"
September 18, 2007

In arguing for greater tools to combat terrorists, you have made statements recently in public concerning some of the significant threats the U.S. faces from foreign powers and terrorists. Specifically, in August, you stated that a significant number of Iraqis have been smuggled across the Southwest border.

1) What further information can you tell us today about those crossings? Are you aware of individuals from other state sponsors of terror that have illegally crossed the Southwest border?

2) Is securing our Southwest border a matter of national security? Do you believe that the Southwest border is sufficiently secure at this point?

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.

OLA-28

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

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.

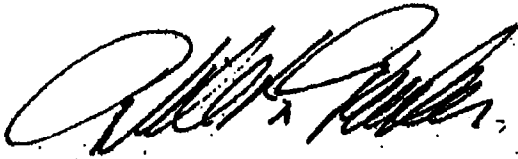
* * * * *

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

Ahmad, Usman

From: Tracci, Robert N
Sent: Friday, February 08, 2008 11:21 AM
To: Cabral, Catalina

Statement of Attorney General Michael B. Mukasey

Before the House Committee on the Judiciary

February 7, 2008

Chairman Conyers, Ranking Members Smith, and Members of the Committee. Thank you for the opportunity to testify about the important work being carried out by the men and women of the Department of Justice and for permitting me to highlight key challenges that lie ahead.

In the short time that I have been at the Department, I have confirmed what I had hoped and expected to find: men and women who are talented, committed, and dedicated to fulfilling its historic mission. That mission is to advance justice by defending the interests of the United States according to the law; to protect Americans against foreign and domestic threats; to seek just punishment for those who violate our laws; to assist our State and local partners in combating violent crime and other challenges; and to ensure the fair and impartial administration of justice by protecting the civil rights and liberties that are the birthright of all Americans.

OLA-30

These values are not only central to the mission of the Department, but defining features of our democracy, and I thank the Committee for its efforts to help realize them.

During my tenure, I have sought opportunities to work with Congress to ensure that the Department is provided the statutory tools necessary to fulfill the Department's crucial mandate. I have also sought to keep Congress apprised of the Department's activities and policy positions where possible, and to respond to the Committee's oversight requests in a spirit of inter-branch comity that respects the institutional interests of the Department and Congress. I pledge to maintain this commitment throughout my tenure as Attorney General of the United States.

I would like to focus on two crucial legislative issues pending before the Congress: the impending expiration of the Protect America Act, and the impending effective date of the United States Sentencing Commission's decision to make a wide range of violent drug offenders eligible for a retroactive reduction in their sentence. I hope to work with Members of this Committee to address each of these problems.

As this Committee is aware, the Protect America Act will soon sunset, but threats to our national security will not expire with it. I urge Congress to pass long-term legislation to update the Foreign Intelligence Surveillance Act (FISA) to ensure that this statute addresses present and emerging threats to our national security.

The Protect America Act is set to expire in just days, and it is vital that Congress enact long-term FISA modernization legislation, with retroactive immunity, before that Act expires. S. 2248, which is a strong bipartisan bill reported out of the Senate Select Committee on Intelligence by a 13-2 margin, is a balanced bill that includes many sound provisions that would allow our Intelligence Community to continue obtaining the information it needs to protect the security of America, while protecting the civil liberties of Americans.

The Department respects the oversight authority of Congress, but sunset provisions create uncertainty in the Intelligence Community and stifle the development of stable partnerships necessary to detect, deter, and disrupt threats to our national security.

I would now like to focus on an issue that will have an impact on community safety nationwide: the Sentencing Commission's decision to apply retroactively, effective March 3, 2008, a new -- and lower -- guideline sentencing range for crack cocaine trafficking offenses.

Unless Congress acts by the March 3 deadline, nearly 1,600 convicted crack dealers, many of them violent gang members, will be eligible for *immediate* release into communities nationwide.

Retroactive application of these new lower guidelines will pose significant public safety risks. Many of these offenders are among the most serious and violent offenders in the federal system and their early release, without the benefit of appropriate re-entry programs, at a time when violent crime has increased in some communities will produce tragic, but predictable results. Moreover, retroactive application of these penalties will be difficult for the legal system to administer given the large number of cases eligible for resentencing, now estimated at upwards of 20,000, and uncertainties as to certain key legal issues remain unresolved.

Let me conclude with the following observation. While differences between this Committee and the Department are inevitable and are consistent with the institutional tension embedded our Founding Document, it is worthwhile to remember what unites us.

We each swear an oath to defend the Constitution of the United States and to uphold the high ideals of public service to which we are entrusted. We must not lose sight of the common goals and common purpose that unify the Department of Justice and Members of the Committee who support its historic and ongoing mission.

Tracking:

Recipient
Cabral, Catalina

Read
Read: 2/8/2008 11:30 AM

Ahmad, Usman



NOT RESPONSIVE

From: Paris, Jeremy (Judiciary-Dem) [mailto:Jeremy_Paris@Judiciary-dem.senate.gov]

Sent: Tuesday, January 29, 2008 2:08 PM

To: Scott-Finan, Nancy; Bookbinder, Noah (Judiciary-Dem)

Subject: RE: Oversight Hearing on January 30th.

The Chairman talked to the AG this morning and they discussed possible questions including torture, DNA grants, OLC opinions, and FOIA reform. I would expect CIA tapes certainly and possibly FISA from some senators.

DLA-35

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

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

Bruce A. Cohen, *Chief Counsel and Staff Director*
Michael O'Neill, *Republican Chief Counsel and Staff Director*

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

OLA-37A

**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?

**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

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?



U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

October 12, 2007

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

Dear Mr. Chairman:

Enclosed please find the corrected transcript of the testimony of Mr. Kenneth Wainstein, Assistant Attorney General, National Security Division, for the hearing held before the Committee on September 20, 2007, concerning the Foreign Intelligence Surveillance Act.

If we may be of further assistance, please feel free to contact this office.

Sincerely,

Brian A. Benzkwski
Principal Deputy Assistant Attorney General

Enclosure

OLA-56A

**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.

OLA-87 A

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?

Ahmad, Usman

From: [REDACTED] ← FOIA EXEMPTION (b)2
Sent: Tuesday, October 30, 2007 8:04 AM
To: [REDACTED] ← FOIA EXEMPTION (b)2
Cc: Benczkowski, Brian A (OLA); Tracci, Robert N; Gerry, Brett (OLP); Potenza, Vito; Greer, John; Reynolds, Patrick; OConnor, Heather Ann; Littlefield, Sean; Brandt, Linda
Subject: RE: meeting with Representative Holt

Good Morning --

FYI, the meeting with Rep. Holt is confirmed for 1000-1200 today, in HPSCI spaces.

Thanks ←

FOIA EXEMPTION (b)2

NOT RESPONSIVE

NOT RESPONSIVE