

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF THE INTELLIGENCE STAFF

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

APR 21 2008

Reference: DF-2008-00017

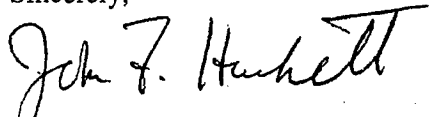
Dear Ms. Hofmann:

This is a final response to your 21 December 2007 letter to the Office of the Director of National Intelligence, wherein you requested under the Freedom of Information Act (FOIA):

“... records from September 1, 2007 concerning exchanges that Director McConnell or other ODNI officials have had with 1) members of the Senate or House of Representatives and 2) representatives of telecommunications companies concerning amendments to FISA...”

We processed your request in accordance with the FOIA, 5 U.S.C. § 552, as amended. Enclosed are 26 documents, totaling approximately 127 pages, that have been found to be responsive to your request. Redactions have been taken on 32 pages pursuant to FOIA Exemptions 1,2,3, and 6, 5 U.S.C. § 552(b)(1), (2), (3), and (6). An additional 11 documents totaling 31 pages are being withheld in their entirety on the basis of FOIA Exemptions 1, 2, 3, 5, and 6, 5 U.S.C. § 552(b)(1), (2), (3), (5),and (6). Pursuant to the Court's April 4, 2008 order attached is an affidavit setting forth the basis for the information being withheld. We anticipate filing a more detailed justification for our withholdings in connection with the Department of Justice's Motion for Summary Judgment if necessary.

Sincerely,



John F. Hackett
Director, Information Management Office



TOP SECRET / [REDACTED] / NOFORN / [REDACTED]

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

FISA Modernization

“Exclusive Means,” the Wyden Amendment, and Immunity

TOP SECRET / [REDACTED] / NOFORN / [REDACTED]



November 5, 2007



The Exclusivity Provision Proposed by
Senator Feinstein

- “Notwithstanding any other provision of law, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which electronic surveillance (as that term is defined in section 101(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(f)), and surveillance authorized under Title VII of such Act, may be conducted.” (*Emphasis added.*)



Intent of FISA

- FISA was intended to govern domestic electronic surveillance activities for foreign intelligence purposes.
- “The committee has explored the feasibility of broadening [FISA] to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude extension of this bill to overseas surveillances.” (H.R. Rep. No. 95-1283, at 27).
- Even where the actual acquisition occurred in the United States, FISA did not intend to cover certain intelligence activities directed overseas.
- “[T]his class of surveillance is among the most sensitive and important class of surveillances this Government conducts in the United States. These factors led the committee to amend [FISA] so as not to require a judicial warrant in this class of surveillances. The fact that Americans’ civil and constitutional rights were not affected by these surveillances, when weighed against even the incremental risk to security by including the courts in the approval process, suggested that the benefits of a warrant requirement is such cases were outweighed by its potential risks.” (*Emphasis added.*) (H.R. Rep. No. 95-1283, at 26).



Wyden Amendment Surveillance of U.S. Persons Overseas

- We are working with the Committee and providing technical assistance.
- The amendment to the section regarding U.S. persons contains numerous technical problems.
 - Use of the term "acquisition of communications" creates uncertainty in how the IC is to treat the incidental collection of U.S. person communications.
 - Contains a contradiction concerning what the FISA Court must find.
 - Will the Court review the probable cause determination of the Attorney General (Sec. 703(c)(2)(B)(i)) or "approve the acquisition" (Sec. 703(c)(2)(B)(ii))?
 - No emergency, transition, or appeal procedures under this provision.
 - Acquisitions that occur in the United States may not target a U.S. person except in accordance with the provisions of Title I.
 - In a few cases, the IC would be unable to obtain a FISA court order under Title I in regard to these activities because the Court has no jurisdiction.



Wyden Amendment U.S. Communications “Reviewed.”

(b) (1)
(b) (3) - 50 USC 403
(b) (3) - 18 USC 793
(b) (3) - P.L. 85-36

- IGs are to review the number of persons located in the U.S. whose communications have been reviewed.





TOP SECRET//SI//NOFORN//NF

Immunity

(b) (1)
(b) (3) - P.L. 86-36

- The Immunity Provision in the SSCI bill is narrowly tailored.
- Case-by-case review where the Attorney General must certify that a company's actions were based on assurances of legality, and
- The court is specifically required to determine whether the Attorney General abused his discretion before immunity can be granted.



TOP SECRET//SI//NOFORN//NF

~~SECRET//NOFORN//20321128~~
DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

DEC 13 2007

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

Dear Representative Hoekstra:

(U) Thank you for your letters of 11 September and 25 October 2007, concerning the public disclosure of certain information. We take seriously our responsibility for the protection of intelligence sources and methods as unauthorized disclosures of classified information undermine our ability to gather vital intelligence to protect the Nation.

(U) As the head of the Intelligence Community (IC), by statute and Executive Order, I may determine, as an exercise of discretion, whether in certain cases the public interest in disclosure of information outweighs the damage to national security. It is always difficult to strike the right balance. During the debate on the Foreign Intelligence Surveillance Act (FISA), in the interest of providing an extensive legislative record and allowing for public discussion of this issue, the IC discussed in open settings extraordinary information dealing with our operations. This will come at a price to our ability to collect vital foreign intelligence. However, to ensure open legislative consideration of this matter, leaders of the IC have gone far further in open discussions than in any other time I can recall in my 40 year intelligence career.

(U) As a result, we understand your concern regarding the difficulty of publicly articulating a response to often unfounded speculation. Despite our best efforts, there remains some confusion in the public discussion of FISA and the Protect America Act (PAA). For instance, some critics claim that the PAA authorizes a number of hypothetical activities that extend beyond the scope of the authority contemplated by Congress. We understand the civil liberties concerns underlying these various claims, but some matters cannot be fully addressed in an unclassified setting. That is why it is incumbent of the IC to demonstrate – through actions as well as words – its commitment to ensuring that any application of the new authority is consistent with the Act and with the protection of the privacy and civil liberties of Americans. Accordingly, and in addition to the numerous classified briefings the IC has given on this subject, the use of the authority is subjected to rigorous oversight by the relevant agencies, by the

UNCLASSIFIED when separated from Attachment

~~SECRET//NOFORN//20321128~~
DRY FROM: COL 3 0

Department of Justice, by my office, and by the Congress. This is not a substitute for public discourse, however, and we appreciate your commitment protecting sensitive sources and methods. Per your request, we are providing guidelines, drafted by the National Security Agency, outlining the parameters of an unclassified discussion of these matters.

(U) Regarding your specific question in both letters concerning my El Paso Times interview, I do not believe I confirmed, nor did I intend to confirm, any specific relationship between the Government and any specific party. We have discussed this matter personally and the Department of Justice has provided a further detailed explanation in court. Their filing is attached and thoroughly discusses the facts made public.

(U) Finally, General Hayden's comments similarly did not expose sources and methods. As was noted in a letter from the Central Intelligence Agency (CIA) dated October 10, 2007, General Hayden's remarks to the Council on Foreign Relations were unclassified and all had been previously released to the public after a rigorous review process. As you are aware, this is a process that was strengthened at CIA over a year ago.

(U) Safeguarding classified information in a free and open society is a daily challenge for the IC. We appreciate your attention to this important issue and look forward to working with you further to protect our sensitive national security information. If you have any questions on this matter, please contact the ODNI Director of Legislative Affairs, Kathleen Turner at [REDACTED] b2

Sincerely,



J. M. McConnell

Enclosures:

cc: The Honorable Silvestre Reyes

11 April 2007

Suggestions on How to Avoid Classified Discussions on FISA Modernization
In an Unclassified Hearing

(SSCI, 17 April 2007)

(U) The staff of the SSCI has requested NSA's recommendations on how to avoid classified discussions in the upcoming hearing on FISA modernization. This paper responds to that request. Topics highlighted in bold below should be avoided in the open session because they are classified. Non-bolded text is unclassified and, therefore, suitable for the open hearing.

FISA MODERNIZATION

(U) The FISA as currently written is not agile enough to handle the broad intelligence needs of the country. Enacted in 1978, it has not kept pace with 21st Century developments in communications technology. As a result, the FISA frequently requires judicial authorization to collect the communications of a non-U.S. person outside the United States. This clogs the FISA process with matters that have little to do with protecting legitimate privacy rights. Modernizing the FISA would greatly improve the FISA process and relieve the massive amounts of analytic resources currently being used to craft FISA orders that have the effect of extending privacy protections to persons not entitled to receive them.

(U) Specifically, the FISA's definition of "electronic surveillance" should be revised so that it no longer matters how collection occurs (whether off a wire or from radio) or where.

(U) The only thing that should matter is the target. If the target of foreign intelligence surveillance is a person reasonably believed to be in the United States or if all parties to a communication are reasonably believed to be in the United States, the Government should have to go to court to obtain an order authorizing such collection. This would return the FISA to what we believe is its original purpose of protecting the civil liberties of persons in the United States.

- (U) Any targeted persons or communications outside the United States that are currently covered by FISA Court orders would be beyond the scope of the amended FISA. Civil liberties would be protected through the application of long-standing minimization procedures.
- ~~(S//NF)~~ Beyond simply stating that the law has not kept up with technology and therefore often requires the Intelligence Community to obtain orders when we are directing surveillance at foreigners overseas, **the Committee should avoid for**

~~Derived From: NSA/CSSM 1-52~~

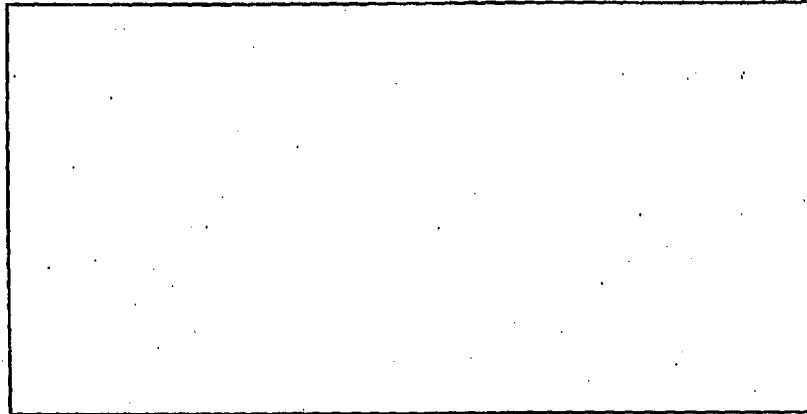
~~Dated: 6 January 2007~~

~~Declassify On: 20391123~~

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~SECRET//COMINT//NOFORN//2009-123~~

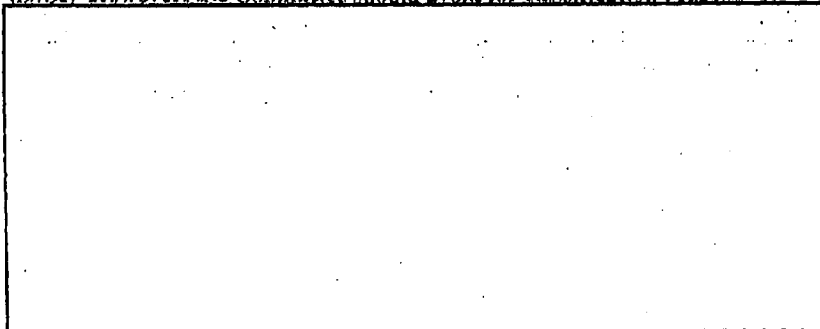
classification reasons all discussions of the technological aspects of electronic surveillance, including:



o Anything else regarding how NSA does collection.

(U) Presently, the Attorney General is authorized to direct a communications carrier to assist the Government with the exercise of electronic surveillance authorized under the FISA. However, the FISA does not provide a means by which the Attorney General can compel cooperation if the private entity is not willing to comply. The FISA should be amended to enhance the authority of the Government to compel cooperation by obtaining a FISA Court order.

• ~~(S//SI)~~ However, the Committee should avoid for classification reasons all



(U) Over time, dealings with the FISA Court have resulted in the secretion of information that now needs to be added to applications for electronic surveillance orders. Supporting these applications has become burdensome and unnecessarily strains analyst resources. The FISA process should be streamlined by, for example, allowing the use of summaries in FISA applications.

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~SECRET//COMINT//NOFORN//2009-123~~

TERRORIST SURVEILLANCE PROGRAM

(U) The President has not renewed his authorization for the Terrorist Surveillance Program. It is currently being conducted under the authority of the FISA Court.

- ~~(S//SI//NF)~~ For classification reasons, the Committee should avoid discussions of operational details of the Program or FISA Court matters.

~~TOP SECRET//COMINT//ORCON//NOFORN~~

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

October 16, 2007

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

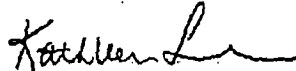
The Honorable Peter Hoekstra
Ranking Member
House Permanent Select Committee on Intelligence
House of Representatives
Washington, DC 20515

Dear Mr. Chairman and Representative Hoekstra:

(U) Attached please find responses to questions resulting from the committee's September 20, 2007, open hearing on the Foreign Intelligence Surveillance Act and Protect America Act. The attached responses are in addition to responses provided to your committee on October 4, 2007.

(U) If you require additional information, please contact me at [REDACTED] b2

Sincerely,



Kathleen Turner
Director of Legislative Affairs

Enclosure: As stated

UNCLASSIFIED WHEN SEPARATED FROM ENCLOSURE

~~TOP SECRET//COMINT//ORCON//NOFORN~~

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

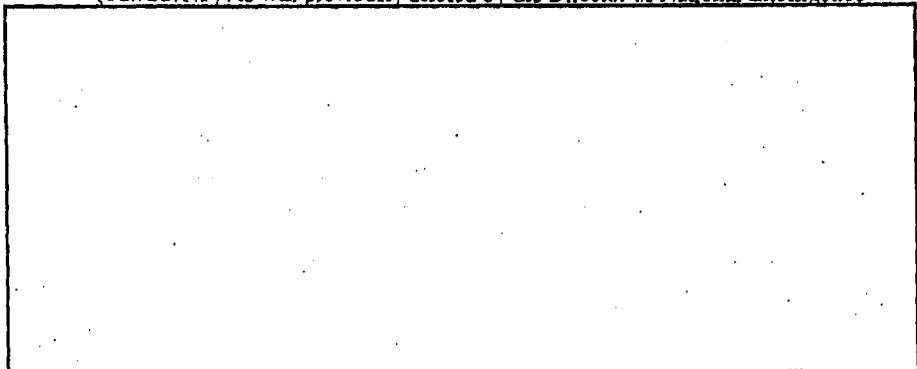
~~TOP SECRET//COMINT//ORCON//NOFORN//20320108~~

Rep. Schakowsky Question: Provide specific instances of how NSA or the intelligence community was prevented altogether from collecting foreign intelligence prior to the passage of the PAA and how H.R. 3356 could or could not have corrected that problem

(TS//NF) Prior to passage of the Protect America Act (PAA), NSA could not collect foreign intelligence off a wire in the United States unless and until it demonstrated probable cause [redacted]

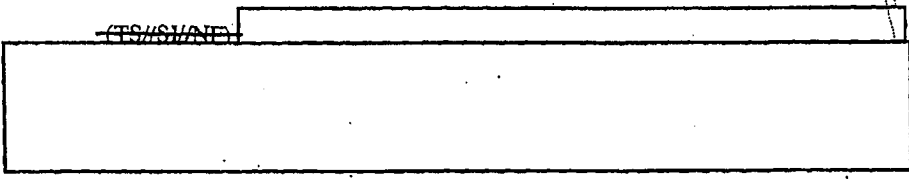
[redacted] NSA's experience has been that this diverted scarce analyst resources and time from data analysis and reporting in order to prepare and obtain FISA orders. As demonstrated in the example provided below, the time spent preparing and obtaining a FISC order also caused delay in [redacted] which effectively meant that important foreign intelligence information was lost until the FISC authorization was obtained, sometimes a matter of days, weeks, or months. More importantly, it is not simply a matter of adding resources to the process. The FISA process has become clogged by extending privacy protections to foreigners overseas who are not entitled to them.

(TS//SI//NF) As was previously briefed by the Director of National Intelligence



(TS//SI//NF) The passage of the PAA allowed NSA to [redacted] for which there was insufficient time or resources to prepare the necessary documentation required to meet the standards of FISA. PAA collection is more agile because the necessary authorization is acquired more rapidly, enabling [redacted] sooner, minimizing the window during which the important intelligence information can be lost.

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36



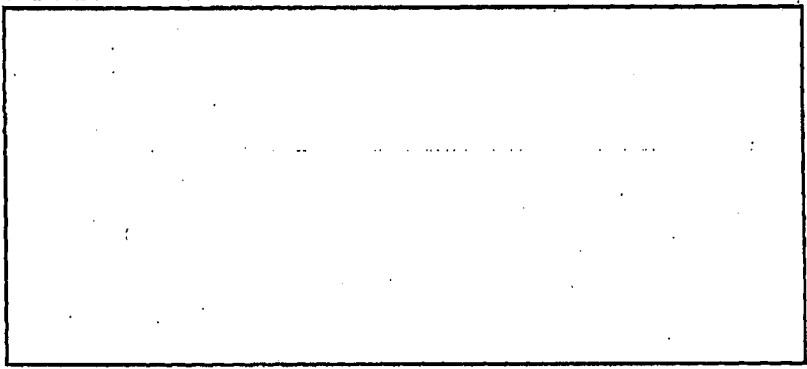
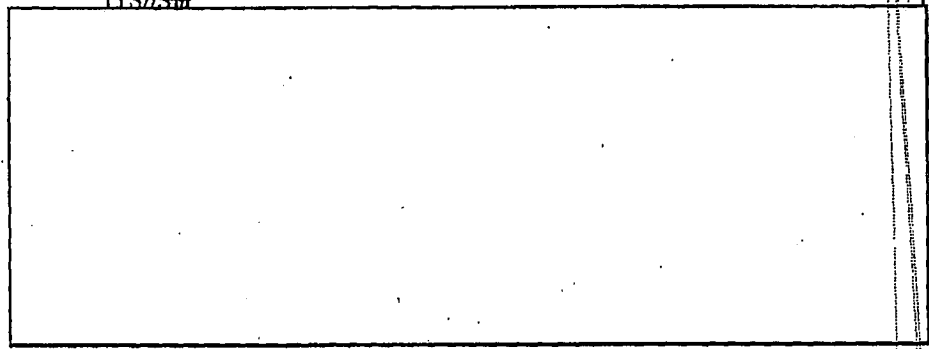
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

~~TOP SECRET//COMINT//ORCON//NOFORN//20320108~~

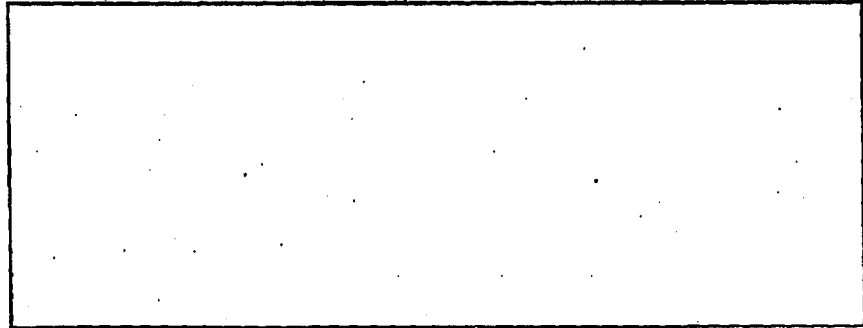
(b) (1)
(b) (3) - 50 USC 403
(b) (3) - 18 USC 798
(b) (3) - P.L. 86-36

~~TOP SECRET//COMINT//ORCON//NOFORN//20320108~~

~~(TS//SI)~~



~~(TS//SI//REL TO USA, FVEY)~~



How could or could not H.R. 3356 correct the problem?

~~(TS//SI//NF)~~ Notwithstanding that H.R. 3356 seeks to make it clear that a court order is not needed to acquire the contents of communications between persons that are located outside the U.S. for the purpose of collecting foreign intelligence information, the bill does not enable NSA to gather foreign-foreign communications in any new way without getting a court order. The language of the pre-PAA FISA already provided that a

~~TOP SECRET//COMINT//ORCON//NOFORN//20320108~~

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~TOP SECRET//COMINT//ORCON//NOFORN//20320108~~

court order is not needed to collect communications from [redacted]
[redacted]

~~(TS//SI//NF)~~ Because any targeting of a U.S.-ended communication without a court order is a violation of the law, and would remain so under H.R. 3356, NSA must be constantly vigilant in its collection efforts to avoid inadvertent violations.

[redacted]

~~(TS//SI//NF)~~ [redacted]
[redacted]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~(U//FOUO)~~ H.R. 3356, unlike the Protect America Act, does not address the issue of communications where one end may be in the United States. The Protect America Act provides that an acquisition in which the target is reasonably believed to be located outside the United States is not within FISA's definition of electronic surveillance, i.e., it focuses on the target not the potential parties to the communication. This has greatly facilitated, as demonstrated in the example above, NSA's flexibility and agility in tracking foreign intelligence targets.

~~(U//FOUO)~~ Section 105(a) of H.R. 3356 also does [redacted]
[redacted] nothing to alleviate the problems described by the DNI to Congress in early August.

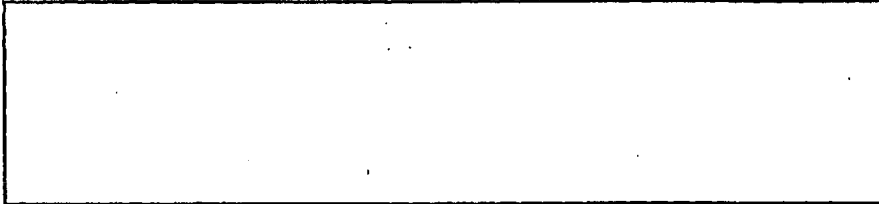
(b) (3)-P.L. 86-36

~~(U//FOUO)~~ Independent of section 105A, section 105B apparently seeks to make it easier for NSA to target individuals outside the United States. [redacted]

[redacted]

[redacted]

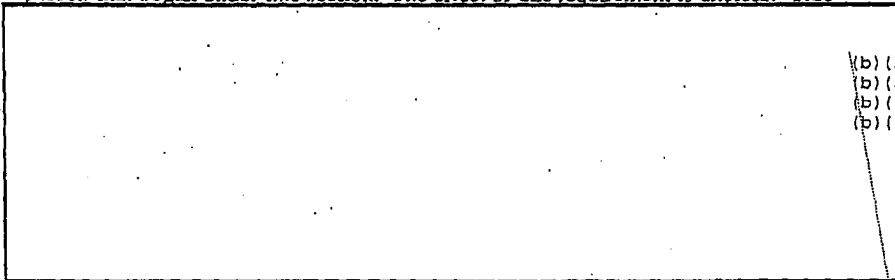
~~TOP SECRET//COMINT//ORCON//NOFORN//20320108~~



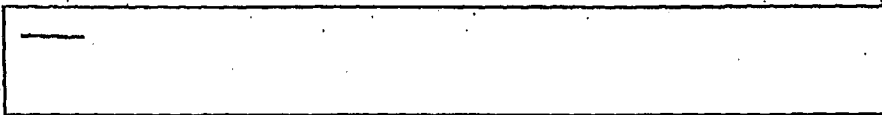
(U//~~FOUO~~) On its face, this would appear to be an improvement to the pre-PAA FISA. However, implementation of the bill would pose significant practical obstacles. First, with regard to the requirements summarized above, although the Government would not be required to identify "the persons, other than a foreign power, against whom electronic surveillance will be directed," it is unclear whether this would permit targeting of individuals who were not themselves tied to/affiliated with a "foreign power" as defined in FISA. Similarly, although specific individuals need not be identified, the court would still be required to make a determination that a significant purpose of the electronic surveillance was to obtain foreign intelligence information. It seems extremely unlikely that the court would be able to make such a determination without an individualized description of the targets and/or their tie to a foreign power.

(b) (1) (S//~~FOUO~~) [redacted] Asking analysts to describe for a judge why the significant purpose of surveillance of individual targets is to produce foreign intelligence information would almost certainly come close to replicating the process under pre-PAA FISA whereby NSA analysts spent their time explaining why there was probable cause to believe that a target was an agent of a foreign power before surveillance was authorized. This alone would make the bill an ineffective means of relieving the problems that the DNI described to Congress prior to passage of the PAA.

(S//~~FOUO~~) [redacted] Additional and even more significant problems exist with regard to requirements imposed after initiation of surveillance. Section 105B (d) imposes a requirement for establishment of guidelines to ensure that a court order be sought to initiate electronic surveillance or continue electronic surveillance of a U.S. person that began under this section. The effect of this requirement is unclear. This



(b) (1)
(b) (3) - 50 USC 403
(b) (3) - 18 USC 798
(b) (3) - P.L. 86-36



(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~TOP SECRET//COMINT//ORCON//NOFORN//20320108~~

[Redacted]

~~(S//SI)~~

[Redacted]

(b) (1)

~~(S//SI)~~ [Redacted] Additional significant practical problems are posed by the requirement for an audit by the DOJ IG every 60 days regarding compliance with the guidelines established under subsection 105B (d): Informing Congress of circumstances where targets of electronic surveillance were subsequently determined to be in the United States, rather than abroad, would be feasible.

[Redacted]

~~(S//SI)~~ [Redacted] Intelligence analysts must comb through extremely large amounts of data to do their job.

[Redacted]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

However, they are prohibited from querying databases of such intercept for communications to, from or about U.S. persons, and can only disseminate information concerning U.S. persons, when it is recognized, in accordance with procedures approved by the Attorney General. Thus, imposition of an audit/reporting requirement such as that included in the bill would essentially turn intelligence analysis on its head, requiring analysts to spend much more time identifying and accounting for incidental intercept of U.S. person communications that they simply ignore in every other context. Furthermore, it is unclear how this requirement could be implemented in any meaningful way.

[Redacted]

[Redacted]

~~TOP SECRET//COMINT//ORCON//NOFORN//20320108~~

[Redacted]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

(b) (1)

(TS//SI) [Redacted] In summary, even if one could draft guidelines that met the requirements of the bill in this area, they would almost certainly impose on NSA analysts a host of requirements for analysis and evaluation of the material [Redacted]

[Redacted] For over 30 years, NSA has developed [Redacted] outside the definitions of electronic surveillance in FISA, and by all accounts, it has handled any incidentally-acquired U.S. person communications in a manner that provides adequate protection for the privacy of these individuals. [Redacted]

[Redacted]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

Rep. Schakowsky Question: How frequently does U.S. person information get collected under the Act?

(TS//SI//NF) NSA Does Not Routinely Measure U.S. Person Information Collected

[Redacted]

[Redacted] there is no way to predict whether the communications of a foreign target will mention a U.S. person or whether someone from the United States may contact or be contacted by that foreigner. In order to ascertain how much U.S. person information NSA has incidentally collected, NSA analysts would have to divert their focus from analyzing the data collected for foreign intelligence purposes and focus on determining, where possible, the extent of U.S. person information that was incidentally included within collected communications. This would consume huge amounts of scarce resources and divert the Agency from fulfilling its foreign intelligence mission.

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

(b) (1)

(S//SI) [Redacted] Analytic Factors: Intelligence analysts must comb through extremely large amounts of data to do their job. [Redacted]

[Redacted]

[REDACTED]

NSA analysts are prohibited from querying Agency databases for communications to, from or about U.S. persons, and can only disseminate information concerning U.S. persons, when it is recognized, in accordance with procedures approved by the Attorney General. Thus, imposition of an audit/reporting requirement such as that which would be required to respond to this question would essentially turn intelligence analysis on its head, requiring analysts to spend much more time identifying and accounting for incidental intercept of U.S. person communications that they simply ignore in every other context. Furthermore, it is unclear how this requirement could be implemented in any meaningful way.

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

[REDACTED]

~~(TS//SI//NF)~~ Specialized Study. That said, NSA is aware of the high congressional interest in the subject of how much U.S. person information is collected under the PAA.

[REDACTED]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~
[REDACTED]

~~(TS//SI//NF)~~
[REDACTED]

[REDACTED]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~ [Redacted]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~ [Redacted]

(U) ~~(S//NF)~~ **More Meaningful Measures of U.S. Person Information Collected:**
A more quantitative and meaningful metric could be derived from the application of our minimization procedures, which are in place to govern the process NSA follows when it collects, processes, retains, and disseminates foreign intelligence to, from, or about a U.S. person. Our minimization procedures, approved by the Attorney General and shared with the intelligence committees, permit the dissemination of information that identifies a U.S. person if that information meets two tests: it is evaluated to be foreign intelligence, and the identifying information is necessary to understand or assess the foreign intelligence information. In the overwhelming majority of cases, however, NSA masks the U.S. identity when we disseminate foreign intelligence in an intelligence report. Consequently, we capture the number of intelligence reports we issue that contain minimized and masked U.S. person information, as well as the number of times SIGINT customers request the minimized U.S. identity. These measures have proven over the years to be an effective way to protect U.S. privacy and are very conducive to regular reporting to our overseers.

Rep Tierney Question: Please submit your complete reason why you thought that the following language wasn't clear enough to satisfy your needs to make it certain that no foreign communications required a warrant? Section 105(a) reads, "Notwithstanding any other provision of this Act, a court order is not required for the acquisition of the contents of any communication between persons that are not located within the United States for the purpose of collecting foreign intelligence information without respect to whether the communication passes through the United States or the surveillance device is located within the United States."

~~(TS//SI//NF)~~ Notwithstanding that Section 105(a) of H.R. 3356 seeks to make it clear that a court order is not needed to acquire the contents of communications between persons that are located outside the U.S. for the purpose of collecting foreign intelligence information, the provision does not enable NSA to gather foreign-foreign

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~TOP SECRET//COMINT//ORCON//NOFORN//20320108~~

communications in any new way without getting a court order. The language of the pre-Protect America Act (PAA) FISA already makes it clear that a court order is not needed to collect communications from [redacted]

[redacted]

~~(TS//SI//NF)~~ Because any targeting of a U.S.-ended communication without a court order is a violation of the law, and would remain so under Section 105(a), NSA must be constantly vigilant in its collection efforts to avoid inadvertent violations [redacted]

[redacted]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted]

[redacted]

~~(U//FOUO)~~ Section 105(a) of H.R.3356, unlike the Protect America Act, does not address the issue of communications where one end may be in the United States. The Protect America Act provides that an acquisition in which the target is reasonably believed to be located outside the United States is not within FISA's definition of electronic surveillance, i.e., it focuses on the target not the potential parties to the communication. This has greatly facilitated NSA's flexibility and agility in tracking topics of foreign intelligence interest.

~~(U//FOUO)~~ Section 105(a) of H.R. 3356 also does [redacted]

[redacted]

[redacted] nothing to alleviate the problems described by the DNI to Congress in early August.

(b) (3)-P.L. 86-36

[redacted]

~~TOP SECRET//COMINT//ORCON//NOFORN//20320108~~

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?

Senator Charles E. Schumer
Written Questions for Director of National Intelligence McConnell
October 2, 2007

1. Engineer Susan Landau, writing in the *Washington Post*, argued on August 9, 2007 that the wiretapping permitted under the Protect America Act (PAA) will create unintended information security risks for the United States. Because the executive branch still requires a warrant to acquire domestic-to-domestic communications, the National Security Agency (NSA) will need to filter these protected communications from those that can be intercepted without a warrant under the PAA. Landau states that the NSA will need to build "massive automatic surveillance capabilities into telephone switches[,] but she warns that creating this infrastructure will mean that "within 10 years, the United States will be vulnerable to attacks from hackers across the globe, as well as the militaries of China, Russia and other nations." Thus, the same technology used by the NSA to protect Americans could potentially be used against us in a cyber-attack.

- a. Do you agree with Ms. Landau's prediction that the executive branch will need to build surveillance capabilities into telephone switches?
- b. If the executive branch does foresee using sweeping collection mechanisms such as Ms. Landau describes, what assurance can you give this Committee that this collection technology will not ultimately be used to attack the United States?

2. Assistant Attorney General Kenneth L. Wainstein, in a letter to Congress on September 14, 2007, reiterated the executive branch's position that a warrant is required when a U.S. person is the target of such surveillance. S. 2011, an alternative bill for modernizing the Foreign Intelligence Surveillance Act (FISA), would have directed the Attorney General to develop his or her own guidelines for obtaining a court order when communications that are acquired without a warrant evolve into a surveillance effort targeted at a U.S. person. The PAA does not direct the Attorney General to develop such consistent safeguards. Will you support adding a provision to the PAA, if it is renewed, that directs the Attorney General to develop consistent guidelines to ensure that the executive branch seeks judicial approval for continuing any electronic surveillance that effectively becomes surveillance of a U.S. person or that infringes on the reasonable expectation of privacy of a U.S. person? If not, why not?

3. You stated at the hearing on September 25, 2007, that the bulk collection of electronic communications would be authorized under the PAA, but only if the communications constitute foreign intelligence. However, another witness, Suzanne Spaulding, later stated that "as a matter of statutory interpretation, [FISA Section] 105A does not require that it have anything to do with foreign intelligence or be for foreign intelligence purposes. It simply defines all of those communications out of those statutory protections. So, it certainly would enable or not put any restrictions on the bulk collection." The application of Section 105B, in contrast, is limited to foreign intelligence information.

- a. Do you wish to clarify your statements at the hearing regarding the extent to which the PAA authorizes the bulk collection of electronic communications, in light of the different language used in Sections 105A and 105B and the view expressed by Ms. Spaulding following your testimony?

- b. Please explain whether there is any operational or other reason why Section 105A refers to all surveillance directed at a person reasonably believed to be outside the United States, while Section 105B is limited to foreign intelligence.

4. The Church Committee of the 1970s, which uncovered abuses of electronic surveillance prior to the passage of FISA, noted that the "inherently intrusive nature of electronic surveillance . . . has enabled the Government to generate vast amounts of information – unrelated to any legitimate government interest – about the personal and political lives of American citizens. The collection of this type of information has, in turn, raised the danger of its use for partisan political and other improper ends by senior administration officials."

- a. Does the executive branch, as a matter of practice, permanently discard, within a certain period of time, electronic communications that are acquired during surveillance but that are found not to contain foreign intelligence information? If so, for what period of time? If not, why not?
- b. What assurance can you give this Committee that information collected through electronic surveillance will be safeguarded from being used for "partisan political and other improper ends" by officials in our current and future presidential administrations?

5. You have repeatedly claimed that minimization rules are sufficient to protect the privacy of U.S. persons whose communications are acquired under the new Section 105B of FISA, added by the PAA. However, public assessment of the adequacy of these rules is difficult because the minimization procedures are classified. Moreover, some observers are concerned that these rules are inconsistently applied. For example, a *Newsweek* investigation found that in just 18 months from 2004 to 2005, the NSA gave out the redacted names of 10,000 U.S. citizens to bureaucrats and analysts. During the hearing before the Judiciary Committee on September 25, 2007, you indicated that you are willing to support annual review of the minimization procedures by the Foreign Intelligence Surveillance Court and by Congress.

- a. Will you support adding a provision to the PAA, if it is renewed, that requires the Foreign Intelligence Surveillance Court to review minimization rules at least annually and to issue a decision on whether the NSA's rules are constitutional and adequate to protect Americans? If not, why not?
- b. Will you also support adding a provision to the PAA, if it is renewed, that requires the Foreign Intelligence Surveillance Court to review minimization rules whenever these rules are revised and to issue a decision on whether the NSA's rules are constitutional and adequate to protect Americans? If not, why not?
- c. Will you also support adding a provision to the PAA, if it is renewed, that requires a periodic independent assessment of whether the intelligence community is complying with the applicable minimization rules? If not, why not?

6. Section 105A of FISA, added by the PAA, provides that FISA's warrant requirement does not apply to surveillance "directed at a person reasonably believed" to be in a foreign country. Section 105B of FISA, added by the PAA, sets out an alternative procedure for surveillance not covered by FISA, but appears to use broader terminology.

Section 105B provides that you and the Attorney General may, on your own authority, direct the collection of intelligence information "concerning" persons reasonably believed to be in a foreign country.

- a. In your interpretation of the PAA, is surveillance "concerning" an overseas person in fact a broader category than surveillance "directed at" an overseas person? Stated differently, do you read the PAA to grant you (with the Attorney General) the authority to order the collection of a broader universe of intelligence information than what is actually exempted from FISA's warrant requirement?
- b. If so, please explain why you advocated for FISA modernization legislation that contains this language.

7. In his letter to Congress of September 14, 2007, Assistant Attorney General Wainstein also stated that the PAA does not authorize warrantless physical searches of the homes or effects of Americans; acquisition of domestic-to-domestic communications; or the collection of medical, library or other business records for foreign intelligence purposes. In order to provide greater clarity and given the Administration's position that the PAA already does not authorize the above activities, will you support adding a provision to the PAA, if it is renewed, that explicitly states that the PAA does not authorize warrantless physical searches of the homes or effects of Americans; acquisition of domestic-to-domestic communications; or the collection of medical, library or other business records for foreign intelligence purposes? If not, why not?

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

DDSI
RELEASE

NEED EQUITIES

SEP 18 2007

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

The Honorable Jerrold Nadler
Committee on the Judiciary
House of Representatives
Washington, DC 20515

The Honorable Robert C. "Bobby" Scott
Committee on the Judiciary
House of Representative
Washington, DC 20515

Dear Mr. Chairman, Representative Nadler, and Representative Scott:

Thank you for your letter of September 11, 2007, regarding your concerns about statements made concerning the Foreign Intelligence Surveillance Act (FISA). I also thank you for the opportunity to discuss with your committee recent amendments to FISA and the critical need to make these changes permanent.

With respect to my interview with the *El Paso Times*, I commented on the subjects covered by that interview to address, at a summary level, important issues concerning legislative proposals before the Congress. In doing so, I balanced the goal of providing additional information on the public record with the need to preserve specific facts vital to our foreign intelligence collection efforts.

In the course of that interview, while discussing the need for legislation that provides liability protection for private sector companies alleged to have assisted us following the events of September 11, 2001, I did not confirm any specific relationship between the Government and any particular company. The Department of Justice has addressed this issue with the courts and their relevant filings are attached.

With respect to FISA applications, my point is that it is not feasible, nor wise, to remove significant numbers of our most critical analytic resources – counterterrorism analysts who understand the languages, organization, and operations of our enemies – from tracking current

1
NSD-10

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

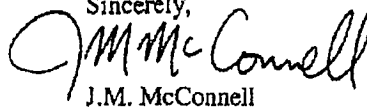
threats to the nation and devote large numbers of them to writing detailed probable cause justifications in cases where the foreign targets are located overseas.

You also inquired about general classification authority. Both statute and Executive Orders provide the DNI with classification and declassification authorities.

Finally, I on 12 September 2007, issued a clarification of the comment made during the Senate Committee on Homeland Security and Governmental Affairs hearing on September 10, 2007. There I discussed the critical importance to our national security of FISA as a long standing statute. The Protect America Act was urgently needed by our intelligence professionals to close critical gaps in our capabilities and permit them to more readily follow terrorist threats, such as the plot uncovered in Germany. However, to be clear, information contributing to the recent arrests was not collected under authorities provided by the Protect America Act.

I am grateful for the time and effort you and other Members of Congress spent working to close the gaps in our intelligence capability prior to the August recess. I look forward to continuing our dialogue and working with you further on this important issue. If you have any additional questions on this matter, please contact me or my Director of Legislative Affairs, Kathleen Turner, who can be reached on [REDACTED] b2

Sincerely,



J.M. McConnell

Enclosures: As stated

cc: The Honorable Lamar S. Smith
The Honorable Trent Franks
The Honorable J. Randy Forbes

February 5, 2008

RELEASENSD *requirements*

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.

NSD-16

The Honorable Harry Reid

S. 2248, reported by the Senate Select Committee on Intelligence, would satisfy both of these imperatives. That bill was reported out of committee on a nearly unanimous 13-2 vote. Although it is not perfect, it contains many important provisions, and was developed through a thoughtful process that resulted in a bill that helps ensure that both the lives and the civil liberties of Americans will be safeguarded. First, it would establish a firm, long-term foundation for our intelligence community's efforts to track terrorists and other foreign intelligence targets located overseas. Second, S. 2248 would afford retroactive liability protection to communication service providers that are believed to have assisted the Government with intelligence activities in the aftermath of September 11th. In its report on S. 2248, the Intelligence Committee recognized that "without retroactive immunity, the private sector might be unwilling to cooperate with lawful Government requests in the future without unnecessary court involvement and protracted litigation. The possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation." The committee's measured judgment reflects the principle that private citizens who respond in good faith to a request for assistance by public officials should not be held liable for their actions. Thus, with the inclusion of the proposed manager's amendment, which would make necessary technical changes to the bill, we strongly support passage of S. 2248.

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

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

I. Limitations on the Collection of Foreign Intelligence

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

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

The Honorable Harry Reid

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

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

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

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

The Honorable Harry Reid

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

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

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

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

The Honorable Harry Reid

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

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

II. Liability Protection for Telecommunications Companies

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

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

The Honorable Harry Reid

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

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

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

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

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

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

The Honorable Harry Reid

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

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

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

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

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

The Honorable Harry Reid

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

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

III. Other Amendments

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

The Honorable Harry Reid

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

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

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

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

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

The Honorable Harry Reid

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

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

IV. Expiration

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

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

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

The Honorable Harry Reid

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

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

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

As we have discussed above, and the Senate Intelligence Committee recognized, "without retroactive immunity, the private sector might be unwilling to cooperate with lawful Government requests in the future without unnecessary court involvement and protracted litigation." As it concluded, "[t]he possible reduction in intelligence that might result from this delay is simply unacceptable for the safety of our Nation." In short, if the absence of retroactive liability protection leads to private partners not cooperating with foreign intelligence activities, we can expect more intelligence gaps.

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

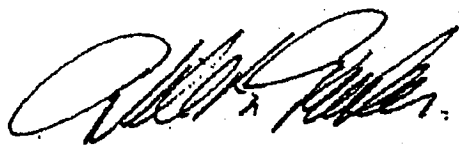
* * * * *

The Honorable Harry Reid

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

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

Sincerely,



Michael B. Mukasey
Attorney General



J.M. McConnell
Director of National Intelligence

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

Attachments

DEP/ODNI

March 6, 2008

The Honorable Pete Hoekstra
Ranking Member
House Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, DC 20515

RELEASE

NSD Equities

The Honorable Lamar Smith
Ranking Member
House Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Congressman Hoekstra and Congressman Smith:

We write in response to your letter of March 5 concerning the core surveillance authorities needed in any modernization of the Foreign Intelligence Surveillance Act of 1978 (FISA). We appreciate the seriousness of Congress's engagement in this critical issue. As you note, much of the recent discussion concerning FISA reform has centered on liability protection for electronic communication service providers who assisted the Government in preventing another terrorist attack after September 11, 2001. The liability protection provisions of the Rockefeller-Bond FISA modernization bill, passed by a strong bipartisan majority in the Senate and now pending in the House of Representatives, provide precisely the protection from civil suits that our national security requires. Although liability protection is critical to any FISA modernization proposal, equally if not more important to our efforts to protect our nation from terrorist attack and other foreign intelligence threats are the carefully drafted authorities that modernize FISA for the technologies of the 21st century. These authorities address the operational aspects of conducting surveillance of foreign terrorists and other threats overseas, and we urge that they not be altered.

Over the past year, the Intelligence Community and the Department of Justice have worked closely with Congress, first to pass the Protect America Act last summer by a bipartisan majority in both the House and Senate as a short-term measure to enable us to close dangerous intelligence gaps and then to create a long-term framework for foreign intelligence surveillance of individuals outside the United States. Those months of bipartisan effort and of careful compromise are reflected in the bill passed by the Senate, a bill that we believe would also enjoy the support of a majority of the members of the House of Representatives. Title I of the Senate bill would preserve the core authorities of the Protect America Act—authorities that have helped us to obtain exactly the type of information we need to keep America safe. For example, the Senate bill would allow the Government to continue collecting foreign intelligence information against foreign terrorists and other foreign intelligence targets located outside the United States without

NSD-3

obtaining prior court approval. Initiating surveillance of individuals abroad without awaiting a court order will ensure that we will keep closed the intelligence gaps that existed before the passage of the Protect America Act.


It is essential to our national security that any legislation passed by the House of Representatives not weaken the intelligence collection authorities provided in the Protect America Act, which are preserved in Title I of the Senate bill. As we have explained in prior correspondence, the RESTORE Act, passed by the House last November, would seriously undermine these authorities and may well reopen the gaps temporarily closed by the Protect America Act. The RESTORE Act, or legislation similar to it, is, in short, no substitute for the bipartisan Senate bill. Even seemingly small changes to the Senate bill may have serious operational consequences. It is our firm belief that the Senate bill provides our intelligence professionals the tools they need to protect the country.

Title I of the Senate bill also protects the civil liberties of Americans. In fact, the privacy protections for Americans in the Senate bill exceed the protections contained in both the Protect America Act and the RESTORE Act. For example, the bill would require for the first time that a court order be obtained to conduct foreign intelligence surveillance of an American abroad. Historically, such surveillance has been conducted pursuant to Executive Branch procedures when, for example, a U.S. person was acting as an agent of a foreign power, e.g., spying on behalf of a foreign government. This change contained in the Senate bill is a significant increase in the involvement of the FISA Court in these surveillance activities. Other provisions of the bill address concerns that some have voiced about the Protect America Act, such as clarifying that the Government cannot "reverse target" without a court order.


The bill substantially increases the role of the FISA Court and of Congress in overseeing acquisitions of foreign intelligence information from foreign terrorists and other national security threats located outside the United States. Under the Senate bill, the Court would review certifications by the Attorney General and the Director of National Intelligence relating to such acquisitions, the targeting procedures used by the Government to conduct acquisitions under the Act, and the minimization procedures used by the Government to ensure that such acquisitions do not invade the privacy of Americans. The bill would require the Attorney General and the Director of National Intelligence to conduct semiannual assessments of compliance with targeting procedures and minimization procedures and to submit those assessments to the FISA Court and to Congress. The FISA Court and Congress would also receive annual reviews relating to those acquisitions prepared by the heads of agencies that use the authorities of the bill. In addition, the bill requires the Attorney General to submit to Congress a report at least semiannually concerning the implementation of the authorities provided by the bill and would expand the categories of FISA-related court documents that the Government must provide to the congressional intelligence and judiciary committees.

We remain prepared to work with Congress towards the passage of a long-term FISA modernization bill that would strengthen the Nation's intelligence capabilities while protecting the civil liberties of Americans, so that the President can sign such a bill into law. Congress has such legislation before it—the bipartisan Senate bill—and the authorities provided in Title I of that bill strike a careful balance and should not be altered.

Sincerely,



Michael B. Mukasey
Attorney General



J.M. McConnell
Director of National Intelligence

cc: The Honorable Silvestre Reyes
The Honorable John Conyers, Jr.

619/0246

Congress of the United States

Washington, DC 20515

RELEASE

NSD Activities

March 5, 2008

The Honorable Michael B. Mukasey
Attorney General of the United States
United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530

The Honorable Michael McConnell
Director of National Intelligence
Office of the Director of National Intelligence
Washington, D.C. 20511

Dear Mr. Attorney General and Director McConnell:

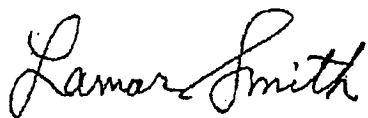
In recent weeks, the focus of the public debate on Foreign Intelligence Surveillance Act (FISA) legislation appears to have unfortunately and simplistically narrowed to one issue – retroactive liability protection for telecommunications companies that assisted the government following the terrorist attacks of September 11, 2001.

We are concerned that this narrowed debate is belittling the significance of the provisions contained in Title I of the FISA Amendments Act of 2008 passed by the Senate last month. Congress began the process of updating FISA over nine months ago when Admiral McConnell informed us of a critical gap in our foreign intelligence gathering capabilities.

The Protect America Act (PAA) provided an immediate, temporary FISA fix. Before Congress enacted the PAA, the intelligence community was “missing a significant portion of what we should be getting” with respect to foreign terrorist communications. Unfortunately, the PAA was allowed to expire nearly three weeks ago, once again degrading the intelligence community’s ability to collect foreign intelligence.

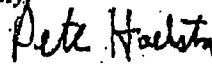
Title I of the Senate-passed bill provides a long-term solution to the foreign intelligence gap. We believe it is important that Members of Congress be fully informed about the importance of Title I to your foreign intelligence operations and we ask you to clarify and comment on these tools provided in the Senate bill.

We appreciate your prompt attention to our request.



Lamar Smith
Ranking Member
House Committee on the Judiciary

Sincerely,



Pete Hoekstra
Ranking Member
House Permanent Select Committee
Intelligence

PRINTED ON RECYCLED PAPER

NSD-4

SI P/ OMI

February 22, 2008

RELEASE

NSD equities

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

Dear Chairman Reyes,

The President asked us to respond to your letter of February 14, 2008, concerning the urgent need to modernize the Foreign Intelligence Surveillance Act of 1978 (FISA). Your assertion that there is no harm in allowing the temporary authorities provided by the Protect America Act to expire without enacting the Senate's FISA reform bill is inaccurate and based on a number of misunderstandings concerning our intelligence capabilities. We address those misunderstandings below. We hope that you find this letter helpful and that you will reconsider your opposition to the bill passed last week by a strong bipartisan majority in the Senate and, when Congress returns from its recess, support immediately bringing the Senate bill to the floor, where it enjoys the support of a majority of your fellow members. It is critical to our national security that Congress acts as soon as possible to pass the Senate bill.

Intelligence Collection

Our experience since Congress allowed the Protect America Act to expire without passing the bipartisan Senate bill demonstrates why the Nation is now more vulnerable to terrorist attack and other foreign threats. In our letter to Senator Reid on February 5, 2008, we explained that: "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." That is exactly what has happened since the Protect America Act expired six days ago without enactment of the bipartisan Senate bill. We have lost intelligence information this past week as a direct result of the uncertainty created by Congress' failure to act. Because of this uncertainty, some partners have reduced cooperation. In particular, they have delayed or refused compliance with our requests to initiate new surveillances of terrorist and other foreign intelligence targets under existing directives issued pursuant to the Protect America Act. Although most partners intend to cooperate for the time being, they have expressed deep misgivings about doing so in light of the uncertainty and have indicated that they may well cease to cooperate if the uncertainty persists. We are working to mitigate these problems and are hopeful that our efforts will be successful. Nevertheless, the broader uncertainty caused by the Act's expiration will persist unless and until the bipartisan Senate bill is passed. This uncertainty may well continue to cause us to miss information that we otherwise would be collecting.

Thus, although it is correct that we can continue to conduct certain activities authorized by the Protect America Act for a period of one year from the time they were first authorized, the Act's expiration has and may well continue to adversely affect such activities. Any adverse

NSD-5

effects will result in a weakening of critical tools necessary to protect the Nation. As we explained in our letter to Senator Reid, 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 of private parties needed to protect our national security;
- The ability to cover intelligence gaps created by new communication paths or technologies.

Our experience in the past few days since the expiration of the Act demonstrates that these concerns are neither speculative nor theoretical: allowing the Act to expire without passing the bipartisan Senate bill has had real and negative consequences for our national security. Indeed, this has led directly to a degraded intelligence capability.

It is imperative that our intelligence agencies retain the tools they need to collect vital intelligence information. As we have explained before, the core authorities provided by the Protect America Act have helped us to obtain exactly the type of information we need to keep America safe, and it is essential that Congress reauthorize the Act's core authorities while also extending liability protection to those companies who assisted our Nation following the attacks of September 11, 2001. Using the authorities provided in the Protect America Act, we have obtained information about efforts of an individual to become a suicide operative, efforts by terrorists to obtain guns and ammunition, and terrorists transferring money. Other information obtained using the authorities provided by the Protect America Act has led to the disruption of planned terrorist attacks. The bipartisan Senate bill would preserve these core authorities and improve on the Protect America Act in certain critical ways, including by providing liability protection to companies that assisted in defending the country after September 11.

In your letter, you assert that the Intelligence Community's ability to protect the Nation has not been weakened, because the Intelligence Community continues to have the ability to conduct surveillance abroad in accordance with Executive Order 12333. We respectfully disagree. Surveillance conducted under Executive Order 12333 in a manner that does not implicate FISA or the Protect America Act is not always as effective, efficient, or safe for our intelligence professionals as acquisitions conducted under the Protect America Act. And, in any event, surveillance under the Protect America Act served as an essential adjunct to our other intelligence tools. This is particularly true in light of the changes since 1978 in the manner in

which communications are transmitted. As a result of these changes, the Government often has been required to obtain a FISA Court order prior to surveillance of foreign terrorists and other national security threats located outside the United States. This hampered our intelligence collection targeting these individuals overseas in a way that Congress never intended, and it is what led to the dangerous intelligence gaps last summer. Congress addressed this issue temporarily by passing the Protect America Act but long-term FISA reform is critical to the national security.

We have provided Congress with examples in which difficulties with collections under the Executive Order resulted in the Intelligence Community missing crucial information. For instance, one of the September 11th hijackers communicated with a known overseas terrorist facility while he was living in the United States. Because that collection was conducted under Executive Order 12333, the Intelligence Community could not identify the domestic end of the communication prior to September 11, 2001, when it could have stopped that attack. The failure to collect such communications was one of the central criticisms of the Congressional Joint Inquiry that looked into intelligence failures associated with the attacks of September 11. The bipartisan bill passed by the Senate would address such flaws in our capabilities that existed before the enactment of the Protect America Act and that are now resurfacing. We have provided Congress with additional and detailed examples of how the Protect America Act temporarily fixed this problem and have demonstrated the operational need to provide a long-term legislative foundation for these authorities by passing the bipartisan Senate bill.

In your letter, you also posit that our intelligence capabilities have not been weakened, because the Government can employ the outdated provisions of FISA as they existed before the Protect America Act. We respectfully disagree. It was that very framework that created dangerous intelligence gaps in the past and that led Congress to pass the Protect America Act last summer.

As we have explained in letters, briefings and hearings, FISA's requirements, unlike those of the Protect America Act and the bipartisan Senate bill, impair our ability to collect information on foreign intelligence targets located overseas. Most importantly, FISA was designed to govern foreign intelligence surveillance of persons in the United States and therefore requires a showing of "probable cause" before such surveillance can begin. This standard makes sense in the context of targeting persons in the United States for surveillance, where the Fourth Amendment itself often requires probable cause and where the civil liberties of Americans are most implicated. But it makes no sense to require a showing of probable cause for surveillance of overseas foreign targets who are not entitled to the Fourth Amendment protections guaranteed by our Constitution. Put simply, imposing this requirement in the context of surveillance of foreign targets located overseas results in the loss of potentially vital intelligence by, for example, delaying intelligence collection and thereby losing some intelligence forever. In addition, the requirement to make such a showing requires us to divert our linguists and analysts covering al-Qa'ida and other foreign threats from their core role—protecting the Nation—to the task of providing detailed facts for FISA Court applications related to surveillance of such foreign targets. Our intelligence professionals need to be able to obtain foreign intelligence from

foreign targets with speed and agility. If we revert to a legal framework in which the Intelligence Community needs to make probable cause showings for foreign terrorists and other national security threats located overseas, we are certain to experience more intelligence gaps and miss collecting information.

You imply that the emergency authorization process under FISA is an adequate substitute for the legislative authorities that have lapsed. This assertion reflects a basic misunderstanding about FISA's emergency authorization provisions. Specifically, you assert that the National Security Agency (NSA) or the Federal Bureau of Investigation (FBI) "may begin surveillance immediately" in an emergency situation. FISA requires far more, and it would be illegal to proceed as you suggest. Before surveillance begins the Attorney General must determine that there is probable cause that the target of the surveillance is a foreign power or an agent of a foreign power and that FISA's other requirements are met. As explained above, the process of compiling the facts necessary for such a determination and preparing applications for emergency authorizations takes time and results in delays. Again, it makes no sense to impose this requirement in the context of foreign intelligence surveillance of targets located overseas. Because of the hurdles under FISA's emergency authorization provisions and the requirement to go to the FISA Court within 72 hours, our resource constraints limit our use of emergency authorizations to certain high-priority circumstances and cannot simply be employed for every foreign intelligence target.

It is also inaccurate to state that because Congress has amended FISA several times, there is no need to modernize FISA. This statement runs counter to the very basis for Congress's passage last August of the Protect America Act. It was not until the passage of this Act that Congress amended those provisions of FISA that had become outdated due to the communications revolution we have experienced since 1978. As we explained, those outdated provisions resulted in dangerous intelligence gaps by causing constitutional protections to be extended to foreign terrorists overseas. It is critical that Congress enact long-term FISA modernization to ensure that the Intelligence Community can collect effectively the foreign intelligence information it needs to protect the Nation. The bill passed by the Senate would achieve this goal, while safeguarding the privacy interests of Americans.

Liability Protection

Your assertion that the failure to provide liability protection for those private-sector firms that helped defend the Nation after the September 11 attacks does not affect our intelligence collection capability is inaccurate and contrary to the experience of intelligence professionals and to the conclusions the Senate Select Committee on Intelligence reached after careful study of the matter. It also ignores that providing liability protection to those companies sued for answering their country's call for assistance in the aftermath of September 11 is simply the right thing to do.

Through briefings and documents, we have provided the members of your committee with access to the information that shows that immunity is the fair and just result.

Private party assistance is necessary and critical to ensuring that the Intelligence Community can collect the information needed to protect our country from attack. In its report on S. 2248, the Intelligence Committee stated that "the intelligence community cannot obtain the intelligence it needs without assistance" from electronic communication service providers. The Committee also concluded 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." Senior intelligence officials also have testified regarding the importance of providing liability protection to such companies for this very reason.

Even prior to the expiration of the Protect America Act, we experienced significant difficulties in working with the private sector because of the continued failure to provide liability protection for such companies. These difficulties have only grown since expiration of the Act without passage of the bipartisan Senate bill, which would provide fair and just liability protection. Exposing the private sector to the continued risk of billion-dollar class action suits for assisting in efforts to defend the country understandably makes the private sector much more reluctant to cooperate. Without their cooperation, our efforts to protect the country cannot succeed.

Pending Legislation

Finally, as you note, the House passed a bill in November to amend FISA, but we immediately made clear that the bill is unworkable and unacceptable. Over three months ago, the Administration issued a Statement of Administration Policy (SAP) that stated that the House bill "falls far short of providing the Intelligence Community with the tools it needs to collect effectively the foreign intelligence information vital for the security of the Nation" and that "the Director of National Intelligence and the President's other senior advisers would recommend that the President veto the bill." We adhere to that view today.

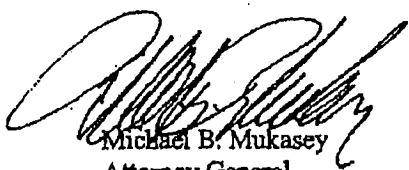
The House bill has several grave deficiencies. First, although numerous senior intelligence officials have testified regarding the importance of affording liability protection for companies that assisted the Government in the aftermath of September 11, the House bill does not address the critical issue of liability protection. Second, the House bill contains certain provisions and serious technical flaws that would fatally undermine our ability to collect effectively the intelligence needed to protect the Nation. In contrast, the Senate bill deals with the issue of liability protection in a way that is fair and that protects the national security. In addition, the Senate bill is carefully drafted and has been amended to avoid technical flaws similar to the ones in the House bill. We note that the privacy protections for Americans in the Senate bill exceed the protections contained in both the Protect America Act and the House bill.

The Honorable Silvestre Reyes

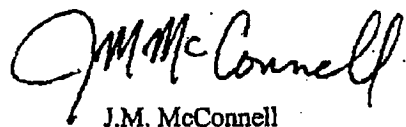
Page 6 of 6

The Department of Justice and the Intelligence Community are taking the steps we can to try to keep the country safe during this current period of uncertainty. These measures are remedial at best, however, and do not provide the tools our intelligence professionals need to protect the Nation or the certainty needed by our intelligence professionals and our private partners. The Senate passed a strong and balanced bill by an overwhelming and bipartisan margin. That bill would modernize FISA, ensure the future cooperation of the private sector, and guard the civil liberties we value. We hope that you will support giving your fellow members the chance to vote on this bill.

Sincerely,



Michael B. Mukasey
Attorney General



J.M. McConnell
Director of National Intelligence

cc: The Honorable Peter Hoekstra
Ranking Member, House Permanent Select
Committee on Intelligence

The Honorable John D. Rockefeller, IV
Chairman, Senate Select Committee on Intelligence

The Honorable Christopher S. Bond
Vice Chairman, Senate Select Committee on Intelligence

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
CIVIL LIBERTIES AND PRIVACY OFFICE

**Civil Liberties and Privacy Provisions of Section 101 of the SSCI FISA Bill S. 2248 --
Review by the ODNI's Civil Liberties and Privacy Office (CLPO), November 2, 2007**

This paper presents a summary of CLPO's review of Title VII of SSCI Bill S. 2248, entitled "FISA Amendments Act of 2007."¹ In particular, this paper focuses on the privacy and civil liberties concerns raised with respect to the Protect America Act (PAA), and identifies the provisions in Title VII of the SSCI bill that address those concerns.²

- **Scope:** Concerns have been raised that section 105A of the PAA could permit surveillance that is not constrained by its provisions calling for assistance by communications providers, and by its foreign targeting and minimization procedures.
 - The SSCI bill addresses this concern by explicitly tying the exercise of new authorities to the protections and limitations set forth in the bill.
- **"Concerning Persons" and Domestic Surveillance.** Concerns have been raised that the PAA could permit surveillance targeting individuals inside the United States – including searches of homes and domestic mail – so long as the purpose was "concerning persons" outside the United States. As explained in a Department of Justice (DOJ) letter dated September 14, 2007, FISA and the Fourth Amendment would not permit such domestic surveillance and physical searches, and the PAA would not be interpreted to in that manner.
 - The SSCI Bill eliminates the "concerning persons" phrase, and incorporates explicit prohibitions against domestic targeting and "reverse targeting" to further assure that the bill only authorizes surveillance that is directed at persons reasonably believed to be outside the United States. It also defines "electronic communications service provider" to more narrowly circumscribe the entities from which assistance must be obtained, and provides that acquisitions must comply with the fourth amendment.
- **Interception of Communications of U.S. Persons.** Concerns have been raised that the PAA could result in the interception of U.S. person communications. As explained in the DOJ September 14 letter, and in a letter by the DNI's Civil Liberties Protection Officer dated September 17, 2007, U.S. persons' privacy interests are protected through "minimization procedures," which must meet FISA's statutory definition. In addition, "reverse targeting" is implicitly prohibited under existing law.
 - The SSCI Bill in addition requires judicial review of minimization procedures and explicitly prohibits reverse targeting. In addition, the bill provides the FISA court with ongoing access to compliance reports and information about U.S. person disseminations and communications, and the explicit authority to correct deficiencies in procedures. The bill also requires annual reviews of U.S. person disseminations and communications and extensive reports to Congress.

¹ It was posted to the SSCI website on October 25, 2007 at: <http://intelligence.senate.gov/071025/s2248.pdf>. This paper reviews only Title VII, Additional Procedures for Targeting Communications of Certain Persons Outside the United States. As such, it does not address other sections, such as those on retroactive immunity. Provisions are paraphrased for space and readability.

² This paper does not purport to take a position on the bill's provisions.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
CIVIL LIBERTIES AND PRIVACY OFFICE

- **Targeting of U.S. Persons Outside the United States.** Concerns have been raised about acquiring information from U.S. persons outside the United States under circumstances where a warrant would be required for law enforcement purposes. Under the PAA, pursuant to longstanding practice, Attorney General authorization would be required under section 2.5 of Executive Order 12333, based on a finding of probable cause that the U.S. person is an agent of a foreign power.
 - The SSCI Bill requires FISA court orders based on probable cause for electronic surveillance of U.S. persons overseas.
- **“Clearly Erroneous” Standard of Judicial Review.** Concerns have been raised about the PAA’s “clearly erroneous” standard of judicial review of the foreign targeting procedures.
 - The SSCI Bill eliminates this standard.
- **Judicial Review of Minimization Procedures.** Concerns have been raised about the absence of judicial review of minimization procedures under the PAA.
 - The SSCI Bill provides for judicial review of minimization procedures.
- **Oversight and Reporting.** Concerns have been raised about the oversight and reporting provisions of the PAA. The PAA requires DNI and DOJ compliance assessments, with reports to the Intelligence Committees. In addition, as explained in the CLPO September 17 letter and in the DNI’s testimony at various hearings, other layers of oversight and reporting exist – and are provided for by law and Executive Order – to supplement the oversight and reporting requirements of the PAA, including by the Inspector General, the Civil Liberties Protection Officer, the Offices of General Counsel for the elements concerned, etc.
 - The SSCI Bill enhances the oversight and reporting requirements by adding provisions relating to Inspector General and agency reviews with respect to certain U.S. person information and communications, and additional reports to Congressional oversight committees.
- **Timing of Court Review.** Concerns have been raised about the timing of FISA court review of procedures – namely, that it takes place after the fact, rather than in advance.
 - The SSCI Bill retains after-the-fact review, but provides that certifications and procedures must be provided within 5 days.
- **Court Role in Overseeing Implementation.** Concerns have been raised about whether the FISA court should have an ongoing role in overseeing implementation of authorities.
 - The SSCI Bill gives the FISA court an ongoing role in overseeing implementation, by providing the court with reports and information regarding compliance with procedures and requirements, and the authority to correct deficiencies or to direct cessation of acquisition.



Classification ~~TOP SECRET//SI//NF~~



U.S. Senate
Select Committee on Intelligence

Fax Cover Sheet

To: J.M. McCOWNELL

From: SENATOR FEINGOLD

SSCI#: 2007-4877

Date: 12/18/2007

Time: 1118

Page 1 of 6

Prepared by: L Shepard

Note to Recipient:

If you did not receive every page of the facsimile, please call
(202) 224-1771.

Classification ~~TOP SECRET//SI//NF~~

DEC. 18. 2007 11:26AM

SSCI

NO. 494

P. 2

RUSSELL D. FEINGOLD
WISCONSIN

508 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5323
(202) 224-1280 (TDD)
rdfeingol@senate.gov

~~TOP SECRET//SI//NOFORN~~

United States Senate

WASHINGTON, DC 20510-4904

COMMITTEE ON THE BUDGET
COMMITTEE ON FOREIGN RELATIONS
COMMITTEE ON THE JUDICIARY
SELECT COMMITTEE ON INTELLIGENCE
DEMOCRATIC POLICY COMMITTEE

SSCI #2007-4877

December 18, 2007

The Honorable J.M. McConnell
Director of National Intelligence
Washington, D.C. 20505

Dear Director McConnell:

(U) I am writing to express serious concerns about the implementation of the Protect America Act and to state my strong disagreement with your assertion, in an op-ed published in the *New York Times* on December 10, that the PAA has "protect[ed] the civil liberties of Americans." Both the procedures set up to implement the PAA, as well as activities conducted thus far, confirm that the Act is fundamentally flawed, particularly with regard to the rights of Americans. I urge you to consider these concerns, both in future implementation of the PAA and as you work to formulate the Administration's position with regard to legislative fixes to these manifest problems.

(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~
[Redacted]

In the absence of an independent assessment, even one based on the "clearly erroneous" standard established by the PAA, it is premature to assert that the PAA is reasonably designed to [Redacted]. Moreover, until the Administration provides recent pleadings and exchanges among the FISA Court, the government [Redacted] Congress cannot even fully assess the extent of the Court's concerns.

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~
[Redacted]

1800 ASPEN COMMONS
ROOM 100
MIDDLETON, WI 53562
(608) 828-1200
(608) 828-1215 (TDD)

517 EAST WISCONSIN AVENUE
ROOM 409
MILWAUKEE, WI 53211
(414) 878-7282

~~TOP SECRET//SI//NOFORN~~
1425 STATE STREET
ROOM 225
LA CROSSE, WI 54601
(608) 785-5887

1040 MAIN STREET
GREEN BAY, WI 54302
(920) 436-7808

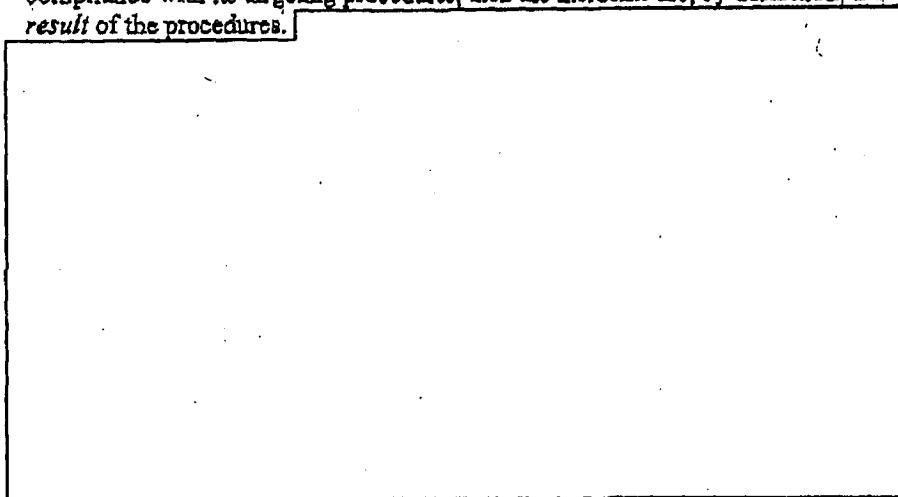
PRINTED ON RECYCLED PAPER

~~TOP SECRET//SI//NOFORN~~

government not only downplays the seriousness of these incidents, but renders the PAA's only Congressional reporting requirement - a semi-annual report on "incidents of non-compliance" - meaningless.

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

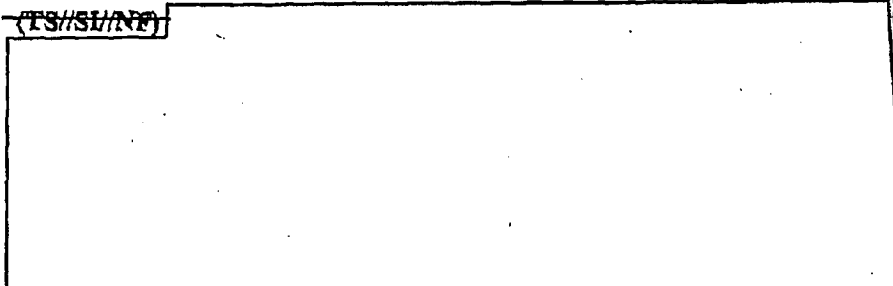
~~(TS//SI//NF)~~ Nonetheless, if the government deems these incidents to be in compliance with its targeting procedures, then the incidents are, by definition, the result of the procedures.



~~(TS//SI//NF)~~ I also have serious concerns about the lack of available information on the number of targeting errors occurring under the new authorities. According to information provided the Committee, oversight conducted thus far has addressed only a sample of the collection conducted by the NSA and the government has not yet conducted a statistical analysis to determine the overall number of targeting errors conducted under the PAA. As the NSA expands the use of its new authorities, the absence of meaningful statistics on the numbers of errors

becomes even more troubling.

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36



~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

[Redacted]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~ I also have concerns about the absence of adequate minimization procedures.

[Redacted]

I do not believe that minimization of U.S. person information adequately protects the privacy of Americans, but even if minimization were theoretically sufficient, it is only as good as the government's ability to actually determine whether it is disseminating U.S. person information.

[Redacted]

It is therefore my position that, as the government dramatically expands the acquisition of communications involving Americans, the checks and balances provided by the FISA Court are critical. However, at a minimum, the government should fundamentally reconsider the presumptions underlying its minimization procedures and establish new procedures relevant to its broad news acquisition authorities.

(b) (3)-50 USC 403
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~

[Redacted]

~~TOP SECRET//SI//NOFORN~~

~~TOP SECRET//SI//NOFORN~~

[Redacted]

Yet, under the PAA, the FISA Court has no role in considering this question, nor has the ODNI Civil Liberties and Privacy Office looked into it.

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~

Although the PAA requires that "a significant purpose of the acquisition is to obtain foreign intelligence information,"

[Redacted]

~~(TS//SI//NF)~~ I have a number of other concerns, based on documents specifically related to the PAA as well as briefings provided the Committee.

[Redacted]

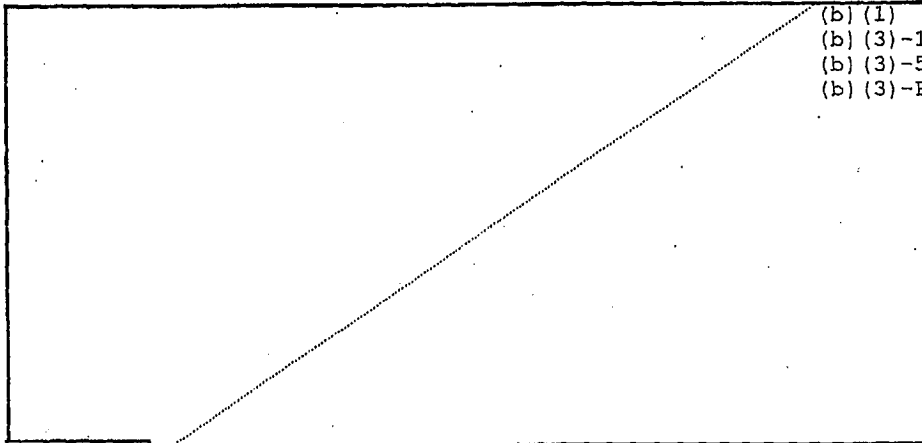
b1

[Redacted]

~~TOP SECRET//SI//NOFORN~~

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~TOP SECRET//SI//NOFORN~~



(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36

Under the PAA, the FISA Court has no role in considering these questions, leaving them entirely to the discretion of the executive branch operating under almost limitless authorities.

(U) The problems described in this letter, many of which raise serious Constitutional questions, can be addressed through legislative fixes. Changes made by the Senate Judiciary Committee to the bill reported by the Senate Intelligence Committee would resolve many of them, as would other amendments currently being considered. Many of these measures will help ensure that collection and analysis is being conducted effectively and that old practices and procedures are brought up to date with the vast amounts of information to be collected under the new authorities. They are also intended to ensure that the government can collect, review, disseminate and use the information it needs to defend our country while protecting the civil liberties of Americans and the checks and balances that come with Congressional and judicial oversight.

Sincerely,

Russell D. Feingold
UNITED STATES SENATOR

CC: The Honorable Michael B. Mukasey
Attorney General of the United States

~~TOP SECRET//SI//NOFORN~~

OCT. 5. 2007 5:04PM

NO. 152 P. 5

CHRISTOPHER S. BOND, MISSOURI, VICE CHAIRMAN
DIANNE FEINSTEIN, CALIFORNIA
RON WYDEN, OREGON
EVAN BAYH, INDIANA
BARBARA A. MIKULSKI, MARYLAND
RUSSELL D. FEINSTEIN, WISCONSIN
BILL NELSON, FLORIDA
SHELTON WHITEHOUSE, RHODE ISLAND

JOHN WARNER, VIRGINIA
CLYDE WAGNER, NEBRASKA
CASSY CHAMBLISS, GEORGIA
DERRY WATSON, UTAH
OLYMPIA J. SNOWE, MAINE
RICHARD BURR, NORTH CAROLINA

~~TOP SECRET//COMINT//NOFORN~~

United States Senate

SELECT COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20510-0475

SSCI #2007-3961

HARRY REID, NEVADA, EX OFFICIO
MITCH MCCONNELL, KENTUCKY, EX OFFICIO
CARL LEVIN, MICHIGAN, EX OFFICIO
JOHN MCCAIN, ARIZONA, EX OFFICIO

ANDREW W. JOHNSON, STAFF DIRECTOR
LOUIE B. TUCKER, MINORITY STAFF DIRECTOR
KATHLEEN P. MASHI, CHIEF CLERK

October 5, 2007

Ms. Kathleen Turner
Director, Congressional Affairs
Office of the Director of National Intelligence
Washington, D.C.

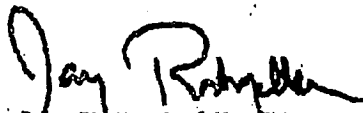
Dear Ms. Turner:


(U) Please extend our appreciation to the Director of National Intelligence, the Director of the National Security Agency, the Assistant Attorney General for National Security, the Deputy Director of the Federal Bureau of Investigation and the other representatives of the Department of Justice and the Intelligence Community who participated in the September 20, 2007 hearing on the implementation of the Protect America Act and amendments to the Foreign Intelligence Surveillance Act.

(U) The Committee has prepared the attached questions for the record resulting from the hearing. We would appreciate you distributing the relevant questions to the appropriate officials in the Intelligence Community and the Department of Justice and providing responses by Friday, October 12, 2007.

(U) Thank you for your assistance. If you have any questions, please contact Ms. Christine Healey, of the Committee staff, at 202-224-1700.

Sincerely,


John D. Rockefeller IV
Chairman


Christopher S. Bond
Vice Chairman

Enclosure
Unclassified when removed from attachment

~~TOP SECRET//COMINT//NOFORN~~

~~TOP SECRET//COMINT~~

QUESTIONS FOR THE RECORD FOR THE HEARING ON
IMPLEMENTATION OF THE PROTECT AMERICA ACT AND FOREIGN
INTELLIGENCE ACT AMENDMENTS
September 20, 2007

Implementation Issues

[REDACTED]

b1

- How many additional certifications are planned under the Protect America Act?
- Will each certification be governed by the identical procedures for determining the reasonableness of "foreign-ness"?
- Do [REDACTED] or any additional certifications that are planned, present different questions in terms of implementation of the Act? Please explain.

b1

2. Mr. Wainstein's statement for the record states that the Department is awaiting the FISA Court's review of the foreign-ness procedures.

- Has DOJ submitted to the Court a formal application to request the Court's review and approval? If so, has this or could this application be shared with the Committee?
- What have been the interactions with the FISA Court to date with respect to that review?
- Has DOJ been given any indication when the Court review will be completed?
- Has the FISA Court issued any orders or opinions since the passage of the Protect America Act that bears on the legislation?

3. Is the NSA the only agency that is now conducting acquisition activities under the Protect America Act?

[REDACTED]

b1

[REDACTED]

b1
b3

~~TOP SECRET//COMINT~~

~~TOP SECRET//COMINT//SI~~

[Redacted]

b1

- How broadly does the scope of the Protect America Act reach in terms of the agencies of government that can be authorized to acquire foreign intelligence information under its terms?

[Redacted]

b1

- Please explain any difference.
- How does [Redacted] meet the requirements for minimization procedures under FISA section 101(h)?

b1

5. [Redacted]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

- Do those procedures require the destruction of the information acquired in these circumstances?

6. [Redacted]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

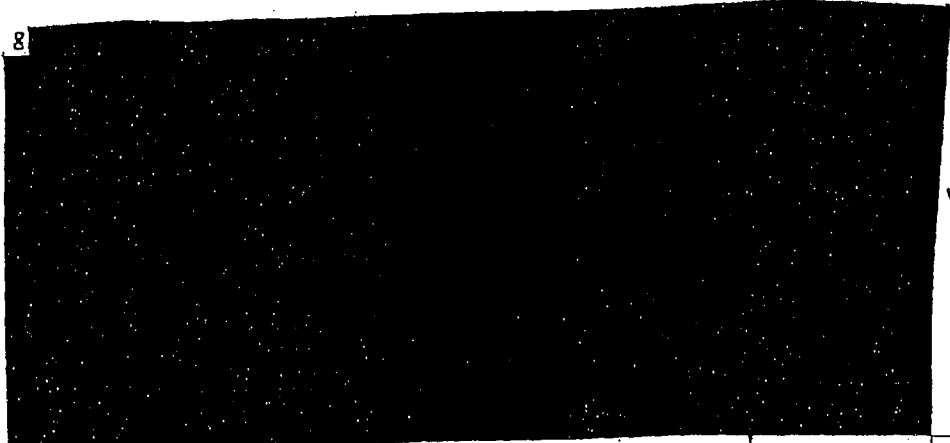
- What law or laws authorize this activity? Is this activity authorized under the Protect America Act based on the usage of the formulation "the acquisition of foreign intelligence information ... [that] concerns persons reasonably believed to be located outside the United States"?

~~TOP SECRET//COMINT//SI~~

~~TOP SECRET//COMINT//NF~~

7. The witnesses testified that the Government will operate under section 2.5 of Executive Order 12333. DNI McConnell said: "To clarify, we are not using the Protect America Act to change the manner in which we conduct electronic surveillance or physical search of Americans abroad." Is it the position of the Department of Justice that the new law could be interpreted to release the U.S. Government from the requirement set forth in section 2.5 that the Attorney General must make an individualized finding that there is probable cause to believe that an American aboard is an agent of a foreign power before the Intelligence Community may conduct electronic surveillance or physical search of that person?

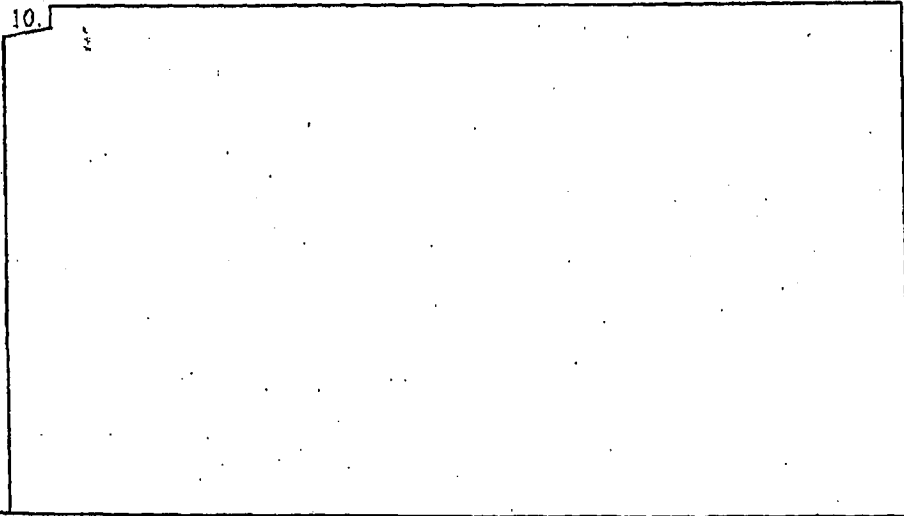
8.



b1.

9. Is there any kind of acquisition which prior to the Protect America Act had been considered to be a search under the FISA which may now be conducted without a FISA search order?

10.



(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

~~TOP SECRET//COMINT//NF~~

~~TOP SECRET//COMINT//NF~~

11. Please provide statistics on the number of communications collected under the Protect America Act that have incidentally captured a U.S. Person communication. Understanding that NSA may not be able to give a precise answer, does the Agency have an estimate on this? If not, is there any way to extrapolate an estimate by looking at other NSA collection programs that target persons outside the United States?

12. For communications where the non-targeted party is a U.S. Person, and that the U.S. Person never himself becomes a target, does the law allow that collection, with minimization, to continue forever? Would you accept a statutory requirement that NSA have an internal review of those communications to make sure that they continue to provide foreign intelligence, that the minimization procedures are applied, and that the U.S. Person is not a target (as such a review already appears to be required by USSID 18, section 5.2)?

13. 

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

14. Please provide copies of guidelines, directives and training materials related to reverse targeting and the determination about "who is the real subject of the surveillance." Please provide copies of any memorandum of law or legal opinions, including OLC documents, and any FISA Court orders, opinions or decisions on this topic with associated pleadings and memoranda of law.

15. Are there any limitations imposed by the PAA on the kind of information collected, so long as the target is overseas? Can the NSA collect business, medical records, library or bookseller, or tax records so long as they are sent by wire to an appropriately selected target?

~~TOP SECRET//COMINT//NF~~

~~TOP SECRET//COMINT//NF~~

16. [Redacted]

(b) (1)
(b) (3) - 50 USC 403
(b) (3) - 18 USC 798
(b) (3) - P.L. 86-36

17. [Redacted]

b1
b3

18. [Redacted]

b1

19. The DNI told Congresswoman Schakowsky that the Intelligence Community would provide information about how much U.S. person information is looked at by an analyst or other person. Please provide the Committee with this information.

20. Under the Protect America Act the Attorney General and the Director of National Intelligence can authorize "the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States." Please explain the intent behind the use of the word "concerning" and what would be the effect of substituting phrases such as "directed at" and "targeting" in its place.

Liability Issues

1. Does the Administration's April proposal to provide liability protection to companies that are alleged to have assisted the nation in the conduct of intelligence activities apply to lawsuits against the United States government or government officials? Please explain.
2. Were the contents of the communications of any plaintiff in any lawsuit concerning the Terrorist Surveillance Program targeted for interception under the Terrorist Surveillance Program?

Streamlining the FISA Process

1. The Administrative Office of the U.S. Courts has submitted to the Congress the recommendation of the FISA Court that it be authorized to meet en banc. One purpose of this change would be to make the Court's decision-making more efficient and predictable as differences among the judges could be resolved more quickly.

- Does the Justice Department have a position on this proposal of the FISA Court?

~~TOP SECRET//COMINT//NF~~

~~TOP SECRET//COMINT//NF~~

WMD Amendment to Definition of Agent of a Foreign Power

1. Mr. Wainstein in his statement for the record highlighted the Administration's request that "the FISA statutory definition of 'agent of a foreign power,' the category of individuals that the Government may target with a FISA court order, be amended to include groups and individuals involved in the international proliferation of weapons of mass destruction."

- Are there any examples of an actual individual involved in the international proliferation of weapons of mass destruction whom the Government cannot bring under surveillance either through a FISA order or the criminal wiretap statutes?
- Are individuals who are suspected of the international proliferation of weapons of mass destruction now considered to be an agent of a foreign government or an international terrorism organization and thus already covered under FISA?
- What would be gained by this proposed amendment that does not exist in current law?

~~TOP SECRET//COMINT//NF~~

UNCLASSIFIED

FISA

Event Key	Date	Event	Subject	Committees	Agencies	Officer
[REDACTED]	09/12/2007	MEMBER MEETING	FISA - DNI MEETING W/ SEN MIKULSKI	SSCI	ODNI	TURNER, KATHLEEN (KATHY)
[REDACTED]	09/18/2007	CMTE BRIEFING-CLOSED	CLOSED BRIEFING ON FISA & THE IMPLEMENTATION OF THE PROTECT AMERICA ACT	SAC/DEF, SA SC, SIC, SSCI	NSA, ODNI	[REDACTED]
[REDACTED]	09/18/2007	CMTE BRIEFING-CLOSED	CLOSED BRIEFING ON FISA & THE IMPLEMENTATION OF THE PROTECT AMERICA ACT	SSCI	NSA, ODNI	TURNER, KATHLEEN (KATHY)
[REDACTED]	09/18/2007	CMTE BRIEFING-CLOSED	CLOSED BRIEFING ON FISA & THE IMPLEMENTATION OF THE PROTECT AMERICA ACT	HAC/DEF, HA SC, HPSCI	NSA, ODNI	[REDACTED]
[REDACTED]	09/18/2007	CMTE HEARING-OPEN	FISA - PROTECT AMERICA ACT IMPLEMENTATION	HIC	DOJ, ODNI	[REDACTED]
[REDACTED]	09/20/2007	CMTE HEARING-OPEN	FISA - OPEN HEARING ON FISA MODERNIZATION	HPSCI	DOJ, ODNI	[REDACTED]
[REDACTED]	09/20/2007	CMTE BRIEFING-CLOSED	FISA - PROTECT AMERICA ACT IMPLEMENTATION		DOJ, NSA, ODNI	[REDACTED]
[REDACTED]	09/25/2007	CMTE HEARING-OPEN	SENATE JUDICIARY COMMITTEE OPEN HEARING ON FISA	SIC	ODNI	[REDACTED]

Total: 8

UNCLASSIFIED

UNCLASSIFIED

b2

FISA

b2

Event Key	Date	Event	Subject	Committees	Agencies	Officer
b2	09/20/2007	CMTE HEARING-CLOSED	CLOSED HEARING ON FISA	SSCI	DOJ, FBI, NSA, O DNI	TURNER, KATHLEEN (KATHY)

Total: 1

UNCLASSIFIED

UNCLASSIFIED

b2

Event Name	Subject	Date	Agencies	Comm.(s)	SubComm.(s)	Status	*****Officer / Atten
<u>MEMBER BRIEFING</u>	CLOSED BRIEFING ON FISA LEGISLATION	11/05/2007	CIA NSA ODNI			SSCI DoJ	[REDACTED] Kathleen P. Turner-DNI-
<u>MEMBER BRIEFING</u>	ALL SENATE BRIEFING ON FISA	12/13/2007					[REDACTED]
<u>MEMBER BRIEFING</u>	ALL SENATE BRIEFING ON FISA	12/13/2007					[REDACTED]
<u>MEMBER BRIEFING</u>	FISA MTG WITH SENATOR FEISTEIN	12/17/2007	DOJ ODNI			SSCI	[REDACTED] Kathleen P. Turner-DNI-
<u>MEMBER BRIEFING</u>	BFNG FOR REPS. BARTON AND UPTON ON FISA AND PRIVATE PARTIES	10/23/2007					[REDACTED] Kathleen P. Turner-DNI-

UNCLASSIFIED

b2

UNCLASSIFIED

Event Name	Subject	Date	Agencies	Comm.(s)	SubComm.(s)	Status	*****Officer / Atte
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
<u>CMTE</u> <u>HEARING-</u> <u>OPEN</u>	FISA AMENDMENTS HEARING	10/31/2007	DoJ			SJC	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
<u>CMTE</u> <u>BRIEFING-</u> <u>CLOSED</u>	FISA RELATED DOCUMENTS	10/30/2007	ONDI			SJC	[REDACTED] Kathleen P. Turner-DNI

b2

b2

UNCLASSIFIED

b2

UNCLASSIFIED

Calendar Entry

Appointment

Notify me

Pencil In

Subject: AG Mtg w/Sen Feinstein

Where: Location: [REDACTED] 62

When: Starts: Mon 12/17/2007 04:30 PM
Ends: Mon 12/17/2007 05:30 PM 1 hour
 Specify additional time


Categorize: [REDACTED]

Description: [REDACTED]

UNCLASSIFIED

Calendar Entry

Appointment

- Notify me 
- Mark Private Pencil In

b2

Subject SSCI Closed FISA Hearing, DIRNSA, DIRFBI, DoJ, Ben Powell, Kathleen Turner (██████████)

Where **Location**


When
Starts: Thu 09/20/2007 02:30 PM
Ends: Thu 09/20/2007 04:30 PM 2 hours
 Specify a different time zone

Categorize

Description

Calendar Entry

Appointment

- Notify me 
- Mark Private Pencil In

62

Subject	Hearing - Senate Judiciary Committee on FISA
---------	--

Where	Location
-------	----------

When	Starts	Tue 09/25/2007	09:30 AM
	Ends	Tue 09/25/2007	12:00 PM
	2 hrs 30 mins		
<input type="checkbox"/> Specify a different time zone			

Categorize

Description

POC: Kathleen

UNCLASSIFIED

Calendar Entry

Appointment

Notify me



Pencil In

ba

Subject Senator Feinstein mtg w/DNI re: FISA

Where [Redacted]

When
Starts: Mon 11/05/2007 02:30 PM
Ends: Mon 11/05/2007 03:30 PM
1 hour
 Specify a different time zone

Categorize [Redacted]

Description [Redacted]

UNCLASSIFIED

~~UNCLASSIFIED//FOUO~~

Calendar Entry

Appointment

Notify me



Mark Private

Pencil In

Subject House Judiciary (OPEN) Hearing on FISA Implementation and Way Ahead (2141 Rayburn)

Where Location

When Starts Tue 09/18/2007 11:00 AM
Ends Tue 09/18/2007 02:00 PM 3 hours
 Specify a different time zone

Categorize

Description

~~UNCLASSIFIED//FOUO~~

UNCLASSIFIED

Calendar Entry

Appointment

Notify me Pencil icon

Subject: All-Senate FISA Briefing

Where: Location: [REDACTED]

When: Starts: Thu 12/13/2007 02:00 PM
Ends: Thu 12/13/2007 03:00 PM 1 hour
 Specify a different time zone

Categorize: [REDACTED]

b2


Description: [REDACTED]

DNI-AG All-Senate FISA Bfng Rescheduled for Thursday, Dec 13, 2-3 pm, [REDACTED]

UNCLASSIFIED

Calendar Entry

Appointment

- Notify me
- Mark Private
-  Pencil In

Subject	HPSCI Open Hearing on FISA w/Kathleen Turner, Ben Powell (1300 Longworth)
---------	---

Where	Location
-------	----------

When	Starts	Thu 09/20/2007	09:00 AM	3 hours
	Ends	Thu 09/20/2007	12:00 PM	
<input type="checkbox"/> Specify a different time zone				

Categorize

Description

Calendar Entry

All Day Event

- Notify me 
- Mark Private Pencil In

Subject Phone Call w/Sen Olympia Snowe re: FISA

Where Location

When
Starts Thu 02/07/2008
Ends Thu 02/07/2008


Categorize

Description

~~UNCLASSIFIED//1000~~

Calendar Entry

All Day Event

- Notify me 
- Mark Private Pencil In

Subject	Phone Call with Sen Blanche Lincoln . re: FISA
---------	---

Where	Location
-------	----------

When	Starts Fri 02/08/2008
	Ends Fri 02/08/2008

Categorize

Description

~~UNCLASSIFIED//1000~~

~~UNCLASSIFIED//1000~~

Calendar Entry

All Day Event

Notify me



Mark Private

Pencil In

Subject	Phone Call w/Sen Bayh re: FISA
---------	-----------------------------------

Where	Location
-------	----------

When	Starts Fri 02/08/2008
	Ends Fri 02/08/2008

Categorize

Description

~~UNCLASSIFIED//1000~~

HEARING OF THE SENATE COMMITTEE ON THE JUDICIARY

Foreign Intelligence Surveillance Act (FISA)
&
Protect America Act

WITNESS:

MR. MIKE McCONNELL, DIRECTOR OF NATIONAL INTELLIGENCE

CHAired BY: SEN. PATRICK LEAHY (D-VT)

LOCATION: 216 HART SENATE OFFICE BUILDING, WASHINGTON, D.C.

TIME: 9:33 A.M. EDT

DATE: TUESDAY, SEPTEMBER 25, 2007

SEN. LEAHY: (Strikes gavel.) Morning.

Before we start, just so everybody will understand, there seems to be - certainly more than I am used to -- people having demonstrations in hearings. Now, just so everybody understands, I want everybody to be able to watch this hearing. I want them to be able to watch it comfortably. If people stand up and block the view of others who are here, they'll be removed. If there's any demonstrations, whether they're for or against a position I might take, for or against a position that Senator Specter might take, for or against the position of anybody else, or the witness, for or against it, they will be removed. I'm sure that's not going to be necessary. I'm sure everybody's going to treat this with the decorum expected. But if somebody's tempted otherwise, the police will be instructed to remove you.

Now, this committee holds this hearing today to consider the Protect America Act that was passed in haste in early August. Congressional leaders went to extraordinary lengths earlier this summer to provide the flexibility Director McConnell said was needed to fix a legal problem with surveillance of targets overseas. I supported a change to FISA, as I've done several times since 9/11. In fact, I think I've supported some 30 changes to FISA since it was written.

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

I do not know who Director McConnell is referring to in his written testimony when he says that he's heard a number of individuals assert that there really was no substantial threat to our nation.

I trust that he's not referring to any senator serving on this committee, but if he did, I hope he'd feel free to say so.

Let me be clear -- I've talked to virtually every senator in this body. Every single senator understands grave threats to our nation. Every single senator, Republican or Democrat or independent, wants us to be able to conduct surveillance effectively. Every senator in this committee voted to give Director McConnell the flexibility he said he needed. So I hope we'll not hear any more irresponsible rhetoric about congressional inquiries risking American safeties. We all want Americans to be safe. Our job is to protect America's security and Americans' rights.

We also take an oath of office, every one of us, to protect America and provide sweeping new powers to the government to engage in surveillance without a warrant of international calls to and from the United States and potentially much more. It does this, in the view of many, without providing any meaningful check or protection for the privacy and civil liberties of the Americans who are on these calls. We are asked to trust that the government will not misuse its authority. When the issue is giving significant new powers to government, "just trust us" is not quite enough.

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

The FISA Court has played an important role ever since the Foreign Intelligence Surveillance Act was passed. It provides a meaningful check on the actions of our government as it's engaged in surveillance on Americans. Unfortunately, the FISA Court was cut out of any meaningful role in overseeing surveillance of Americans in the Protect America Act. The Rockefeller-Levin measure, by contrast, would have allowed the basket surveillance orders if the administration says they're needed and Director McConnell says they're needed, with no individual probable cause determinations but at least had the FISA Court issuing those orders to communications carriers after reviewing the administration's procedures. The Protect America Act, the one that was passed, requires U.S. telecommunications carriers to assist with surveillance just on the say-so of the attorney general and the director of National Intelligence; that's a mistake. It's an invitation to abuse. So I look forward to hearing from the director on what he believes the problems are with the role for the FISA Court issuing orders, how we can create the necessary authority to include the appropriate checks and balances. The problem facing our intelligence agencies is targeting communications overseas. We want them to be able to intercept calls between people overseas with a minimum of difficulty. What changes the equation and raises the stake is that the people may be innocent Americans or they may be talking to innocent people here in the United States. International communications include those of businesspeople or tourists; they even include the families of our troops that are overseas.

We can give the government the flexibility it needs to conduct surveillance of foreign targets, but we can do it while -- with a better job of protecting the privacy of individual Americans.

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

inspector general audit, and I'd like to know why Director McConnell rejected that idea.

In addition, the Protect America Act contains language that appears to go far beyond what the administration said it needed. It redefines electronic surveillance in a way that has expansive implications but was not necessary to accomplish the administration's stated objectives. It has language in many places that at the very least is inscrutable.

It could be read to allow much broader surveillance than the administration has acknowledged or for that matter, I hope, intends. And if this was unintentional, well, then we can fix it. That is one of the things the sunset requires us to do, is look at it. If it was not, then we need to evaluate what was really intended and why.

I know the skilled and dedicated employees of our intelligence agencies want to protect our country, as every one of us do. But if our history has taught us anything, it is that the government cannot and should not be left to police itself when it comes to the secret surveillance of Americans. The founders knew it. The Congress that passed the Foreign Intelligence Surveillance Act knew it.

So I hope this hearing will help us institute the proper protections to safeguard our security and our valued freedoms. As I said, we've amended FISA about 30 different times since it was enacted. Many of us have served here long enough on this committee to have voted for every one of those changes.

Senator Specter.

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

And the congressional response to the administration's requests really depend largely on trust. And the sequence of these warrantless wiretaps has strained that trust relationship because the administration put into effect a program for warrantless wiretaps different from the tradition of applying to a judge, showing probable cause to get judicial authorization for a wiretap, not disclosed to Congress until the newspapers broke the story in December of 2005 when we were in the middle of the final stages of debate on the Patriot Act. Delayed the passage of the Patriot Act, almost scuttled the Patriot Act.

And my response at that time was that the administration at least had confided in the chairman of the Judiciary Committee and the ranking member -- I was then chair, Senator Leahy ranking -- and similar ranking/chairs on other key committees. But the administration chose not to do so, and that kind of a policy, I think, needs to be revisited.

Then when you came forward, Mr. Director, in late July and advised the Congress about the threats which you posed, the chatter which was being undertaken, it was in reliance on your representations that the legislation was enacted.

And it is really vital that we not wait until the last minute to make another hasty decision. We carefully sunsetted the provisions for warrantless

wiretaps directed at people overseas for a six-month period of time. When you talk about some public disclosure or some public understanding of threats to the nation, it's obvious we're in a very difficult situation because you can't -- you're the director of National Intelligence, you can't say too much, and perhaps much of it has to be transmitted to the key committees in a closed session.

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

When we talk about targeting overseas and targeting foreigners overseas, there is a significant difference between targeting people in the United States wiretaps, and I'm glad to see that the administration finally brought the issue for targeting Americans in the United States to the FISA Court.

We struggled with many hearings in the 109th Congress and finally, came to that conclusion. When you are targeting overseas, I think there has to be a sharp distinction between targeting U.S. citizens overseas and targeting others. Right now there is an executive order, which requires the attorney general to find probable cause before a U.S. person is targeted overseas, and my thinking is that the statute ought to be modified to put that responsibility in the FISA Court to establish probable cause, which is the equivalent of authority to issue a warrant if targeting is being directed at U.S. persons.

The administration has argued that the FISA Court ought to be limited just as to procedures, that the administration requires that flexibility. I believe we need more of a showing by you, Mr. Director, of the need for that flexibility and the elimination of the supervision of the FISA Court. The elimination of it has to be justified by real necessity for your flexibility, and I believe it is not sufficient for the FISA Court to be taking a look at procedures every year. I'm not sure how often it ought to be, perhaps every few months, but I think when the renewal is made to the FISA Court even as to procedures, there ought to be a showing as to what you have accomplished, what this invasion of privacy no matter whose privacy is involved has produced some results. So we're going to be weighing these factors very carefully.

One final comment. There's been discussion as to the participation of your counsel in this matter. You called me; I know you've discussed it with a number (of) members of the committee, and Senator Leahy and I have discussed it. And if you have a legal issue and need the advice of counsel, my judgment would be that you ought to have significant latitude. You are not a lawyer. If you need an interjection by a legal counsel, I think you ought to be able to do that, too, but we'll have to make those judgments as the specific questions arise. You have some lawyers on the panel who -- including the chairman, myself, Senator Hatch, Senator Kennedy; Senator Feinstein's smarter than most of the lawyers on legal issues because of her heavy study of the matter. She cites more sections and more codes than anybody else on the committee.

And the senator from Maryland is also an attorney, so we'll be watching very closely to make sure that you have an adequate opportunity to

respond or get assistance on the very complex legal issues which are involved here.

Thank you, Mr. Chairman.

SEN. LEAHY: Thank you.

And as I told Senator Specter earlier this morning when we discussed this, I have written to Director McConnell and thanked him for his offer of having government witnesses and lawyers here to testify too. Of course they have not submitted testimony, and so I declined. We're dealing more with factual issues than legal issues, and we'll be going through those at the -- among others but at the time of the attorney general nomination hearing.

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

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

SEN. ORRIN HATCH (R-UT): Mr. Chairman?

SEN. LEAHY: So would you --

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

SEN. LEAHY: We'll have plenty of time for them to do that. And should the administration want them to come up and testify on the legal thing, we'll try to find a time so they can do just that in the normal forum, with their testimony provided to you and me and everybody else on the committee ahead of time. Admiral --

SEN. HATCH: Well, my only point, Mr. Chairman, is that some of us would benefit from perhaps some legal answers from government officials, because we'll get some from other witnesses and we ought to at least be able to judge that.

SEN. LEAHY: If they wish to -- if the administration wishes to have -- come up, be sworn and testify, we can probably arrange that for them.

SEN. HATCH: Thank you, Mr. Chairman.

SEN. LEAHY: Please stand and raise your right hand.

Do you solemnly the testimony you give in this matter will be the truth, the whole truth, and nothing but the truth, so help you God?

MR. MCCONNELL: I do.

SEN. LEAHY: Thank you.

Director McConnell, we have your full statement. Of course it will be made part of the record. And so we can get into questions, would you please summarize it as you see fit, and we can get into questions.

MR. McCONNELL: Oh, thank you, Chairman Leahy, Ranking Member Specter, and other members of the committee. Thank you for inviting me to appear today. I appreciate the opportunity to discuss the 2007 Protect America Act and the need for lasting modernization of the Foreign Intelligence Surveillance Act that we'll refer to in the hearing, I'm sure, as FISA.

Before I begin, I need to note that some of the specifics that support my testimony cannot be discussed in open session. I understand and I am sensitive to the fact that FISA and the Protect America Act and the types of activities that these laws govern are of significant interest to the Congress and to the public, and for that reason, I will be as open as possible, but much of the substance of these discussions comes with some degree of risk. This is because open discussion of specific foreign intelligence collection capabilities causes us to lose those very same capabilities. Therefore, on certain specific issues, I'd be happy to discuss with members in a classified setting.

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

SEN. LEAHY: As there are things that we should be doing in closed session, I'll confer with Senator Specter, and I'm sure he and I can arrange such a closed session.

MR. McCONNELL: Thank you, sir.

It is my belief that the first responsibility of intelligence is to achieve understanding to provide warning. As the head of the intelligence community, it is not only my desire, it's my duty to encourage changes to policies or procedures and where needed legislation to improve our ability to provide warning of terrorist or other threats to the country. On taking up this post, it became clear to me that our foreign intelligence collection capabilities were being degraded. I had learned that collection using the authorities provided by FISA continued to be not only instrumental but vital in protecting the nation; however, due to changes in technology, the wording of the law, as it was passed in 1978, was actually preventing us from collecting foreign intelligence information. I asked what we could do to correct the problem, and I learned that a number of my colleagues had already been working on the issue. In fact, in July of 2006, the director of NSA, General Keith Alexander, and the director of CIA, General Mike Hayden, testified before this committee regarding proposals to change and update FISA. That 2006 testimony contains significant information and insight into our capabilities and the needs for changes to wording in the law.

I also learned that members of the Congress in both chambers and both sides of the aisle, to include this committee, had proposed legislation to modernize FISA in 2006. A bill passed the House last year, but it was not taken up by the Senate. Therefore, the dialogue on FISA has been ongoing for some time. It's been a constructive dialogue, and I hope it continues in furtherance

of serving a nation to protect our citizens, both their safety and their civil liberties. None of us want a repeat of the 9/11 attacks, even though al Qaeda has stated their intention to conduct such attacks.

As is well-known to this committee, FISA is the nation's statute for conducting electronic surveillance and physical search for foreign intelligence purposes. When passed in 1978, FISA was carefully crafted to balance the nation's need to collect foreign intelligence with the need for the protection of civil liberties and privacy rights of our citizens. There were abuses of civil liberties from the 1940s through the 1970s that were galvanized by the abuses of Watergate that led to the action that caused the Congress to craft and pass the legislation that was signed by President Carter in 1978. This 1978 law created a special court, the Foreign Intelligence Surveillance Court, to provide judicial review of the process.

The court's 11 members devote a considerable amount of time and effort to FISA matters, while at the same time fulfilling their district court responsibilities, and we are indeed grateful for their service.

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

It is my steadfast belief that the balance struck by the Congress in 1978 was not only elegant. It was the right balance to allow my community to conduct foreign intelligence while protecting American civil liberties. Why did we need the changes that the Congress passed this past August? FISA's definition of electronic surveillance simply did not keep pace with technology, and therein is the issue. The definition of electronic surveillance from the 1978 law did not keep pace with technology. Let me explain what I mean.

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

When the law was passed in 1978, almost all calls were on a wire and almost all -- in the United States -- and almost all international calls were in the air or known as wireless communications. Therefore FISA was written in 1978 to distinguish between collection on a wire and collection out of the air. Today, the situation is completely reversed. Most international communications are on a wire, fiber optics, and local calls are in the air.

FISA was originally -- FISA originally placed a premium on the location of the collection. That's a very important issue for us to consider. Therefore collection against a foreign target located overseas, because of the wording in the law, from a wire located in the United States required us to have probable cause standards to seek a warrant from the FISA court to collect against terrorists located overseas.

SEN. LEAHY: But Director, you've emphasized, over and over again, the 1978 law. It has been amended about 30 times since then, around 8 times, 7 or 8 times, at the request of the administration with which you serve. And I

think it's somewhat disingenuous to keep referring to the fact that we were dealing with a 1978 law. It has been dramatically changed since that time.

Now you've testified a number of times over the past few weeks. I know that it's difficult. We all appreciate the time you've taken. But I have -- just as I have concerns with you talking as though we're dealing with a '78 law, I have concerns about some of the statements you've made in those hearings.

For example, two weeks ago in Senate testimony you claimed that information obtained as a result of the Protect America Act, the latest change in the FISA Act, was important to investigation of the recent German terror plot. You said it several times. But later after press reports and members of Congress questions, you issued a statement saying your testimony was not true; the information you spoke of was obtained before the latest law was act and was obtained under the old FISA authority. In the same hearing, you warned if we lose authority in the new legislation, you'd lose 50 percent of our ability to track, understand, know about these terrorists. A week later when you testified before the House Judiciary Committee, that 50 percent had moved to two-thirds of our capability, and in that same hearing, your -- you said you're concerned about losing authority would shut us down. So you went from 50 percent to 100 percent in no time whatsoever.

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

MR. McCONNELL: Sir, when I was asked about FISA and the situation in Germany, the question that I understood was referring to FISA. This panel is making a differentiation between FISA and the Protect America Act. In my mind that's all one act passed in 1978, as you've mentioned several times, updated any number of times. In my view, it was updated in August as the most latest review.

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

SEN. LEAHY: But you can understand -- and I appreciate your explanation of what did appear to be misleading to most people. But you see, if a well-intentioned person like you can make such mistakes, you can understand why we need to have some checks on this so that mistakes are not made. We all believe conducting surveillance on terrorism is vital. I voted to give you greater flexibility on that, as did everybody on this committee, when the matter came before us early August. We -- some of us didn't vote for the Protect America Act, but we voted for the Rockefeller-Levin amendment alternative. It would have given the same flexibility, but it would have had some oversight by the court and more requirements for the executive branch to protect privacy.

When you testified in the past few weeks -- and it sounded like you were saying that here -- you always warn about the dangers of going back to the old FISA process with individual probable-case determinations. But let's be honest, neither the Rockefeller-Levin bill nor the similar House alternative would have required that. I discussed this with you many times. I said I'm not asking for that. Nobody was asking for that.

So I don't know why we keep hearing about legislation that few, if any, members have proposed or supported. I'd like to keep our focus on the Protect America Act and those parts that concern this committee. So as soon we do not propose going back to individual probable-cause determinations by the FISA Court -- as you seem to imply, and nobody -- certainly I've never heard it from any senator -- for overseas targets and not U.S. persons, if we're not going back to individual probable-cause determinations, wouldn't that help you?

MR. McCONNELL: That's exactly the point, Senator. Not having to be required to do probable-cause justification to conduct surveillance against a known terrorist overseas is the whole point. That --

SEN. LEAHY: But nobody's suggested that. We talked about programmatic with -- even with the emergency time you have, after-the-fact determinations. What I worry about when I hear you testify, when I hear the president give his Saturday morning speech, it's -- they're always talking about this 1978 bill. I mean, that's like saying -- if you go out with your brand-new car and say, "Boy, I remember the problems I had with my 1978 car." It's not the same one. It may be the same make of car, but it's a big difference.

MR. McCONNELL: Senator, all I can respond is to say I wish some of those 30 changes that you're mentioning had in fact addressed this issue. Now, this is not a new issue to this committee, as --

SEN. LEAHY: But the Rockefeller-Levin did not require individual probable case.

SEN. HATCH: Mr. Chairman, can we let him finish the statement. I mean, I --

SEN. LEAHY: Would you let the chairman finish his question, please.

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

SEN. LEAHY: (Inaudible) -- and we'll give you plenty of time to --

SEN. HATCH: But let the man finish his statement.

SEN. LEAHY: -- to give the administration's position.

But the Rockefeller-Levin did not require that individual probable cause, did it?

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

The specific question you're asking about, quite frankly, I haven't found a member on the Hill that disagrees with what you're saying. I agree with it; you agree with it. The issue is, we have to get it in legislation in a way that allows us to do -- carry out our mission.

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

SEN. LEAHY: Well, you know, it's interesting. I was in many of those meetings with you and the White House when we talked about (what was going?) and we talked about what we were going to do. None of the concerns that you're talking about now were raised at that time. They were raised -- they were suddenly raised when it's on the floor, and that's what creates the concern. And part of that we'll have to go into classified session to talk about, but I -- you can understand why people worry about this. We have a respected lawyer in Vermont, Robert Gensburg. He and I served as prosecutors at the same time.

He's representing a client being held in Guantanamo Bay. He's worried that his calls regarding his client are being monitored by the government. He makes calls overseas, including to Afghanistan, on behalf of his client.

Now, I'm not going to ask you whether his telephone is being tapped, because I wouldn't expect you to answer that. But you can see why people worry. And I think with Mr. Gensburg, whom I happen to know, or anybody else, they would feel considerably more confident if they thought that the FISA court at least had some oversight here.

My time is up, and I'll yield to -- but you and I should probably discuss that matter in a classified.

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

SEN. LEAHY: And I'm trying to avoid going into the specifics of what we did.

MR. MCCONNELL: And I don't intend to go there, but I need to make three points for this committee so that everybody understands. When I entered back into active duty service and looked at this issue, it appeared to me we had to make some fundamental changes, all the changes to FISA previously notwithstanding. Three points I tried to make, and I gathered the lawyers around me to say, I don't know exactly the wording of how we do this, but here are the three points.

We are disadvantaged because we're currently being required to have a warrant against a foreign target located overseas, and it inhibits our capability to do our job. So we've got to fix that, whatever the wording, the proper wording is. The second is, we have to have a way to compel the private sector to assist us, and to provide a reasonable level of liability protection for them.

So first point: no warrant against a foreign terrorist overseas; compel the private sector to help us. And a third point: This is very important. It's very important to me; it's very important to members of this committee. We should be required; we should be required in all cases to have a warrant any time there is surveillance of a U.S. person located in the United States.

I think that was the intent of the '78 law. That's what was included in the Protect America Act passed in August. That's where we need to be. And anything else we do to that, we have to examine what the words mean to our effectiveness. And so that's where we are with regard to examining this law. So my point to the administration of the Congress is, we need those three points and we need to have them passed in a way that's effective for us to carry out our mission.

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

But I'll yield to Senator Specter.

SEN. SPECTER: Director McConnell, picking up on those three points --

SEN. JEFF SESSIONS (R-AL): Mr. Chairman, just briefly, did the witness ever finish his statement? I don't know if he got to finish his statement. I know you interrupted him.

SEN. LEAHY: He --

SEN. SESSIONS: You had something you were concerned about. But I don't think he got to finish.

SEN. LEAHY: Well, he was at that time several minutes over, and I was trying to give him --

SEN. SESSIONS: His light was green. I noticed it was green when you were asking him that question.

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

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

SEN. LEAHY: I'll guess I'll give the senator --

SEN. HATCH: He ought to be able to get --

SEN. LEAHY: The senator from Utah will have as many rounds as he wants to. If he wants to have 20 rounds to ask the director those questions, we'll give him those.

SEN. HATCH: I'd rather have him out watching over us from a security standpoint than here, to be honest with you.

SEN. LEAHY: Senator Specter.

SEN. SPECTER: And now we return to Director McConnell.

SEN. LEAHY: (Chuckles.)

SEN. SPECTER: Going to the -- if we could start the clock at seven minutes, I'd appreciate it.

SEN. LEAHY: At seven minutes.

SEN. SPECTER: Going to the three issues that you have raised, the surveillance of U.S. persons in the United States --

MR. McCONNELL: Yes, sir.

SEN. SPECTER: -- is now governed by the warrant procedure --

MR. McCONNELL: Yes, sir, it is.

SEN. SPECTER: -- application to the FISA Court, probable cause --

MR. McCONNELL: In all cases is.

SEN. SPECTER: -- before there is wiretapping or surveillance on a person in the United States. Correct?

MR. McCONNELL: (Inaudible.)

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

MR. McCONNELL: That's correct, yes, sir.

SEN. SPECTER: Satisfactory.

I think on our revisiting the statute, we will not call for your certification, Mr. Director, which we did because of our concern about the then attorney general, (but then lodge ?) that in the attorney general. We had some criticism that in giving the authority for certification to the director of National Intelligence, we're letting the fox guard the chicken house. And we did that because we trusted you as the prime assurance, but we can go back to the attorney general now. That'll be acceptable to you, won't it?

MR. McCONNELL: Yes, sir. I'd prefer that.

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

MR. McCONNELL: Yes, sir, it is.

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

But as I said in my brief introductory remarks, there's great value in telling the American people, to the extent possible consistent with national security, what the threat is. When you and I talked in July at length, there was public disclosure of the, quote, "chattering," which was similar to what had occurred prior to 9/11, 2001. Correct?

MR. McCONNELL: Yes, sir.

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

MR. McCONNELL: The level of dialogue and chatter increased significantly. We released, as you recall, a National Intelligence Estimate at about the same time to try to capture the threat from that point three years forward.

SEN. SPECTER: And what do you mean by chatter?

MR. McCONNELL: When we are observing activity of foreign targets highly engaged in what they're doing and what their planning might be and so on, we just refer to that as "chatter", indicating volume.

So that level of volume had increased, and it caused us to be concerned. We combined current activity with the assessment that I was about to mention that we completed after about a year of attempting to develop it and get it coordinated and so on. The timing of the assessment coming out is it was just ready, and July had no -- you know, we didn't speed it up or slow it down to meet any particular timeline; it was that's when it was ready.

And what had happened is we had observed al Qaeda in the Federally Administered Tribal Area of Pakistan be able to re-establish a safe haven that allowed them to have the senior leadership recruit middle-grade leadership, recruit operatives and to train the operatives, and the operatives were being trained in things like commercially available components for explosives. And so that level of activity had increased significantly. The intent of al Qaeda's leadership was to move those operatives from the training area into Europe and into the United States and that was our concern, is our ability to recognize --

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

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

SEN. SPECTER: Anything besides the chatter and the activity in Pakistan which led you to believe they had the capacity to come to the United

States, perhaps, through Europeans who did not need visas, anything beyond that
--

MR. McCONNELL: That's --

SEN. SPECTER: -- that you can disclose publicly?

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

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

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

MR. McCONNELL: They do. One of our concerns has been the level of public activity. I don't know if you follow it that closely, but Osama bin Laden personally has now put out a video and two audio pronouncements over the last month or six weeks, and that's unusual. He had been absent from the airwaves for well over a year. So when we see that much activity at one time, our concern is it's a signal. It's a(n) indication of activity.

So while chatter continues, training continues, recruitment continues, I think probably the easiest way to capture most recent events was the takedown in Germany of what's referred to as IJU, Islamic Jihad Union, which is an affiliate group that trained in Pakistan with al Qaeda and trained the operatives that were arrested in Germany and Pakistan.

SEN. SPECTER: I'm going to back on the second round for the question about giving the FISA Court authority when U.S. persons are targeted overseas instead of the executive order, which now gives that to the attorney general.

MR. McCONNELL: Yes, sir.

SEN. SPECTER: I'll come back to that to see if would be acceptable. But I want to just close the loop on what you've just testified to by asking you, how heavily do you weigh the Osama bin Laden public pronouncements where they disperse him on video -- how heavily do you weigh that as a threat, and why do you weigh that as a threat?

MR. McCONNELL: Sir, it's one of many factors, and I would say it's a concern. It just causes us to be concerned and vigilant. These other factors that I mentioned are the ones that cause me greater concerns. So you can look at over time, and a statement may or may not mean something; there's some -- some have put more credence in it, so I'd say I'm concerned. But when I can see with sufficient detail recruitment and training and explosives designed and that sort of activity, and you follow it over time, you can -- you would understand

why we're concerned. And I would be happy to go in detail if we could go to closed session.

SEN. SPECTER: Thank you.

SEN. LEAHY: Thank you, Senator Specter. And of course if after this that there are members who want a closed session on the Republican side, please talk with Senator Specter about that, and the Democratic side, talk with me, and Senator Specter and I would consult and come to an agreement on that.

Senator Kennedy.

SEN. EDWARD M. KENNEDY (D-MA): Thank you very much, Mr. Chairman, and thank you for having this hearing. Welcome.

Just to review old ground for just a moment. In 1976, in the wake of the fact that we had widespread wiretapping during the previous administration during the Nixon administration, then-Attorney General Levi, a Republican with a Republican administration, asked a number of the members of this committee down to the Justice Department to say we have a real challenge on national security, enormously sensitive information, not only with regard to embassies but with regards to matters that were taking place overseas as well, enormously sensitive.

There was a sense that that attorney general understood that the members of our committee and the members of the Congress are as concerned about national security as anyone within the administration.

And during that period of time, on four different occasions, members of this committee went down to the Justice Department. And when the final legislation was submitted, enacted, in 1978, there was one dissenting vote, one dissenting vote. They worked -- we worked with a Republican administration and a Republican attorney general to try and get the national security issues correctly.

Up comes Mr. Gonzales. The members of this committee said -- many of us who have been through the 1978 experience -- "We want to work with you. We are as concerned about national security as you are." He said, "We don't need your help. We don't need your assistance. We don't need your involvement. And as a matter of fact, we're not even going to tell you what's going on."

Now, I want to have some idea of which tradition you follow on. Are you willing to work with this committee? I mean, do you have sufficient confidence in both the members of this committee that they are concerned about the security as you are and also as concerned about rights and liberties of the American people? When we have -- get it right from an intelligence point of view, we're going to get it right with regards to protecting our rights.

MR. McCONNELL: I do agree with that, Senator. Absolutely.

SEN. KENNEDY: Well, are you going to be working with this committee?

MR. McCONNELL: Absolutely.

SEN. KENNEDY: And can you give us the assurance that whatever is passed by this committee is going to be THE -- and only limit in terms of the intelligence gathering; this is going to be the one -- the new legislation

affirm that the FISA is the sole means by which the executive branch can intercept communications in the United States?

MR. McCONNELL: Sir, the -- if we can get the law that we've just passed made permanent and address the other issues, then that's how I would intend to carry out this program.

SEN. KENNEDY: Well, this is the issue, because there are -- members of the committee aren't sure what the law is. You're going to explain in detail what that law is and what it covers, either in open or in closed session?

MR. McCONNELL: Yes, sir, I'd be happy to do that.

SEN. KENNEDY: Wholly and completely?

MR. McCONNELL: Completely. Wholly and completely.

SEN. KENNEDY: Thank you. Could I go -- ask you a question about the attorney general certification for immunity from liability in the -- for carriers? Isn't it true that the carriers who act pursuant to a warrant or the attorney general's certification already have immunity from liability?

MR. McCONNELL: I don't know the answer to that, sir. I can consult with counsel. I just don't know.

SEN. KENNEDY: It -- well, it's my understanding -- I see the counsel -- did you hear the -- that if the carriers act pursuant to a warrant or attorney general certification, already have immunity from liability?

MR. McCONNELL: That -- under the new law, that's correct. Yes, sir.

SEN. KENNEDY: Was that true under the old law, too?

MR. McCONNELL: I don't know about the old law.

SEN. KENNEDY: All right. Okay. I'll try -- okay. Well, that's --

MR. McCONNELL: What we asked for in the new one was to get that and it was --

SEN. KENNEDY: So if the warrantless surveillance program was legal, as you have claimed, what do carriers need immunity from?

MR. McCONNELL: I'm not sure I understand your question, sir.

SEN. KENNEDY: Okay. Well, why do they -- if they've been abiding by the law, they shouldn't need immunity; if they've been abiding by the attorney general's -- getting a certification, they shouldn't need immunity; so why does the administration ask us to grant immunity for past activities which we have no idea what they were -- at least, I don't think any of the members of this committee know what they -- what possibly they were, but we're being asked to grant that, and that's what I'm trying to driving at.

MR. McCONNELL: Well, going forward, there is postscriptive liability for anyone that would assist us in this mission. In a retroactive sense, those who were alleged to have cooperated with us in the past are being sued, and so it's to seek liability protection from those suits.

SEN. KENNEDY: Well, there is also a desire retroactively to grant -- retroactive immunity.

MR. McCONNELL: That's correct. Yes, sir.

SEN. KENNEDY: The point that is made is that this might bankrupt some of the companies if they go ahead. It's a bad precedent, I think, that we finally have a law and then the carriers are able to violate the law and think that some time in the future they can get immunity by talking about bankruptcy; there are different alternative ways of doing it. There are damages, there's a limit to damages, but it's an important policy issue and question.

And I'll -- let me be contact with you about this so we have -- you have a full idea of what I'm sort of driving at as we try to get --

MR. McCONNELL: I understand.

SEN. KENNEDY: -- because it is complicated, and I know that you want to get the right position on this.

Mr. Chairman, my time is just about up now. I'll come back in a --

SEN. LEAHY: Thank you. Senator Hatch.

SEN. ORRIN G. HATCH (R-UT): Well, Mr. -- or Admiral McConnell, the problem here is is that there were legal opinions that warrantless surveillance could be undertaken, and these companies patriotically cooperated with the government based upon those opinions. Is that a fair statement?

MR. McCONNELL: Yes, sir.

SEN. HATCH: Okay. So the fact that there were no warrants, because it was a warrantless surveillance, should not subject them to litigation.

MR. McCONNELL: Those that were alleged to have helped us were responding to requests from the government that was official, yes, sir.

SEN. HATCH: Did you consider that response a patriotic response or --

MR. McCONNELL: Certainly, sir. Coming out of 9/11 -- and, you know, a lot of things happened where people wanted to be helpful and supportive and so on, so that's the period when it's in question was, how would we understand and be able to push back this threat after the heinous events of 9/11?

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

MR. McCONNELL: Yes, sir.

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

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

SEN. HATCH: And to protect us as citizens in this country.

MR. McCONNELL: There have been a series of things that are not public; a few are -- have become public, but there are many more that have not become public where we've been effective in shutting down something because with -- this program.

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

MR. McCONNELL: Yes, sir. SEN. HATCH: And we enacted it, and it passed somewhat overwhelmingly in the United States Senate.

MR. McCONNELL: Yes, sir.

SEN. HATCH: You don't have any axes to grind, do you? I mean, you're not a -- really a political person, is my understanding.

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

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

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

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

MR. McCONNELL: Yes, sir, it is. Because of the change in technology, our access to communications -- the place and the method, because of the wording of the law, really forced us then to give Fourth Amendment protection to a foreign terrorist.

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

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

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

MR. McCONNELL: Yes, sir, and that goes far beyond just the terrorists. I was just referring to terrorists.

SEN. HATCH: So all you're asking for is the ability to be able to protect the people in this country.

MR. McCONNELL: Yes, sir. SEN. HATCH: And you're aware of an ongoing onslaught of efforts to try and hurt this country and to try and hurt our people, in fact, kill our people. Is that correct?

MR. McCONNELL: Indeed, yes, sir, yes.

SEN. HATCH: This isn't just some little, itty bitty problem, is it?

MR. McCONNELL: No, it isn't.

SEN. HATCH: It's widespread.

MR. McCONNELL: Yes, sir.

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

MR. McCONNELL: Sir, that assertion's made, but the mission of this community is foreign intelligence. And so if there was such targeting, it would have to be for a foreign intelligence purpose.

SEN. HATCH: That's right. But however, the intelligence community is bound by Executive Order 12333.

MR. McCONNELL: Yes, sir.

SEN. HATCH: It's critical for the public to understand that you are still bound by that executive order, and nothing in the Protect Act changed this. Is that correct?

MR. McCONNELL: That's correct, yes, sir.

SEN. HATCH: Now, can you elaborate on the significant and necessary restrictions from Section 2.5 of this executive order, and how they provide protection for the privacy of American citizens overseas?

MR. McCONNELL: Under 2.5, you would be required to produce probable cause standard. In this case, it is reviewed and approved by the attorney general.

SEN. HATCH: That's a protection that have in --

MR. McCONNELL: Yes, sir.

And in the situation, just to get perspective, I think in the past year that happened 55 times, maybe 56, but in the 50s, and the situation was such that someone is either -- they'd been determined to be an agent of foreign power, operating with a foreign power, or a terrorist, or in some cases it might

be a dual citizen. So while someone had U.S. citizenship, they had foreign citizenship too, so that it would put it in that category, where we have to develop probable cause.

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

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

MR. McCONNELL: Yes, sir.

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

SEN. HATCH: By "sleeper," you mean a sleeper cell of terrorists.

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

"There were gaps between NSA's coverage of foreign communications and the FBI's coverage of domestic communications that suggest a lack of attention to the domestic threat. Prior to 9/11, neither agency focused on the importance of identifying and ensuring coverage of communications between the United States and suspected terrorists located abroad."

That's exactly what happened with some of the terrorists here. They were calling known terrorists overseas, and we missed that information.

The joint congressional inquiry concludes:

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

So what we're describing here in this joint commission was a review after the fact of what we should have done.

And the argument that I'm making for the committee today is preserving the legal foundation for us to target the foreigners, foreigners that might call into the country to activate a cell, or a cell that's in the country reaching out to coordinate with a foreign terrorist cell located overseas.

So our community is only targeting the foreigner overseas. Now, some will say, well, wait a minute, there's a situation where you could target overseas when your real target's in the United States. That's a violation of the Fourth Amendment. It's unlawful. So in that case, if we wanted to target or needed to target somebody in the United States, we get a warrant. And so from the way I think about it, it leaves the flexibility to do our foreign intelligence mission, we have a situation under the law to deal with a foreign threat in the United States, and that's all warranted coverage.

SEN. HATCH: My time's up, Mr. Chairman.

SEN. LEAHY: Thank you.

Senator Feinstein.

SEN. DIANNE FEINSTEIN (D-CA): Thank you very much, Mr. Chairman.

Welcome, Director McConnell.

MR. McCONNELL: Thanks, ma'am.

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

MR. McCONNELL: Senator, you and I've discussed this before.

SEN. FEINSTEIN: Right. I just want to go on the record with --

MR. McCONNELL: Yes, ma'am.

SEN. FEINSTEIN: -- what you said to me.

MR. McCONNELL: This is how I would execute this authority under the authorities that I hold. But what you're addressing is a constitutional issue, the difference between Article I and Article II. I --

SEN. FEINSTEIN: What I'm asking for is a yes or no --

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

SEN. FEINSTEIN: Okay.

Under -- Senator Hatch mentioned Executive Order 12,333, Section 2.5, which we have talked about previously. This section applies to any time the intelligence community tries to get information about a U.S. person overseas and requires that the attorney general make a prior finding that there's probable cause to believe that the U.S. person is an agent of a foreign power.

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

MR. McCONNELL: Ma'am, I wouldn't object. What I would ask is we receive the language and examine it, you know, across the table from each other to understand its impact. And so long as it doesn't have unintended consequences, I would have no objection.

SEN. FEINSTEIN: For the subset of Section 2.5, operations where the collection is done inside the United States, would you support shifting the probable-cause determination from the attorney general to the FISA Court?

MR. McCONNELL: It's inside the United States, ma'am. Even today it is under the FISA Court.

SEN. FEINSTEIN: Thank you very much.

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

MR. McCONNELL: If recognized, minimization would require them to expunge it from the database.

SEN. FEINSTEIN: Do the minimization procedures require that U.S. person information is made anonymous before it is disseminated as intelligence reporting? MR. McCONNELL: Yes, ma'am, it does.

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

MR. McCONNELL: Yes, ma'am, and located inside the United States, yes, always.

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

MR. McCONNELL: Back on the minimization procedures, let me give you an example, if I may. If two foreigners are discussing a member of this body, we would have -- that's a U.S. person, so we would have to determine how we would deal with that. So we would -- if it had foreign intelligence value -- we could be being targeted or whatever -- it's our obligation to report that. So we would report it as U.S. Person One or, if there was a second person involved, U.S. Person Two. So the attempt is to protect the identity of the U.S. person when it's done in a foreign intelligence context.

SEN. FEINSTEIN: All right let me just clarify that. When the pickup is being analyzed and a determination is made, that there is intelligence value, by the analyst, exactly what happens?

MR. McCONNELL: The report would be written, and the identity of a U.S. person would be, as I mentioned, listed as U.S. Person One, U.S. Person Two.

SEN. FEINSTEIN: And then what is the warrant?

MR. McCONNELL: If, for whatever reason, the U.S. Person One or Two -- say they were terrorists and they become subject of a target or subject of surveillance, then we would be required to get a warrant.

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

MR. McCONNELL: It would always happen that way. Think of it this way.

SEN. FEINSTEIN: So that is the trigger.

MR. McCONNELL: It's, where do you -- what do you target? If you target -- think of it as a phone number. If you put that phone number in the database as a target, you would have to have a warrant.

SEN. FEINSTEIN: All right, and that is determined, as I understood it previously, when the analyst makes a finding that there is intelligence value.
MR. McCONNELL: That's a way to phrase it. Let's say that -- let's just use a sleeper cell as an example. Foreign terrorist, which is your target, calls into the country and makes contact with somebody who's an accomplice or maybe a sleeper. At that point, you would flag that information for the FBI, so the FBI could get a warrant to conduct surveillance for that person.

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

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

MR. McCONNELL: They already have done that, and I wouldn't have any objection to them looking at the process --

SEN. FEINSTEIN: If that were written into the law?

MR. McCONNELL: Ma'am, right now I have to take it one step further, because we get into unintended consequences. Depending on the phrasing and the way it's captured in the law, it could put us in a position that we couldn't do foreign surveillance, because we can't tell who that person's going to call. We can't control that until we got review beforehand. So if you -- if it's interpreted that way or could be interpreted that way, it would cause us a great difficulty.

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

SEN. FEINSTEIN: Yes, here -- let me summarize it, and we've talked about this before. But it is my position that any collection against a U.S. person abroad with the minimization process, that that process should be approved by the court prior. And you've agreed to that, and that --

MR. McCONNELL: Ma'am, you just mixed two things.

That's why this gets so complex.

SEN. FEINSTEIN: How have I done that?

MR. McCONNELL: All right. You went from targeting a U.S. person abroad to minimization -- two different issues.

SEN. FEINSTEIN: A U.S. person abroad is minimized.

MR. McCONNELL: No, ma'am. Let's say a U.S. person abroad is a dual citizen, agent of foreign power. Currently, what the executive order says is the community would have to produce probable-cause standards, information, but you take that to the attorney general for a warrant. Now, if you're --

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

MR. McCONNELL: All right. So -- all right. So we have -- we're talking about inadvertent collection --

SEN. FEINSTEIN: That's correct.

MR. McCONNELL: Now what the question is, am I objecting to or --

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

MR. McCONNELL: The -- first of all, you may not even realize it's in the database because you do lots of collection. You have to have a reason to look. And you look at it -- if it's foreign intelligence, it is treated the way we discussed; if it's now recognized it's incidental, it would be expunged from the database. Those procedures have been reviewed by the FISA Court. I would have no objection to them looking at them again.

SEN. LEAHY: Senator --

SEN. FEINSTEIN: My time is up. Thank you, Chairman.

SEN. LEAHY: It is, and Senator Coburn is next. SEN. TOM COBURN (R-OK): Thank you, Mr. Director, for being here, and thank you for your service.

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

Can you speak to that for a moment?

MR. McCONNELL: Yes, sir, I can. It's -- we've been doing this for 29 years. It is reviewed at four tiers, four different levels. The agency doing it is -- they have a training process inside, then it's looked at by their general counsel and their IG. My office, as the overseer of the community, we review it. The Department of Justice also reviews it. The FISA Court reviews it for the process and so on, and then it is subject to review by the Congress and the Oversight Committee. So if there's a question and they want to look at, you know, what we've done or what the procedure or visit NSA or look at any of that, we'd make it all available so people could see it and understand it.

SEN. COBURN: Okay. And so that brings me to my next question. You all don't operate without oversight, correct?

MR. McCONNELL: No, no, sir, we don't.

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

MR. McCONNELL: Primarily, it's the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.

SEN. COBURN: Okay. Can you kind of give us a short summary of the oversight mechanisms of the Protect American Act (sic/Protect America Act) that are in place today?

MR. McCONNELL: Yes, sir. The four tiers I just mentioned: internal is for the agency; external, meaning my office and the Department of Justice, the FISA Court and the Congress. We -- since the law was passed in July -- I'm sorry -- in August, and we put our -- we came back up on our full coverage, there have been approximately seven visits -- no, I'm sorry -- 10 visits out to NSA to sit down with the analysts and look at the data and the process, and what's the training standard, what are the conditions and what would you do with the information, and track it through the process.

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

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

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

MR. McCONNELL: Yes, sir. I personally have been very, very public on this issue, criticized in some cases for being so public. But if you'll remember the three points that I started with -- no warrant for a foreigner overseas -- a foreign terrorist located overseas, a way to get assistance from the private sector; the third point is the one I believe very, very strongly in. Any time there is surveillance of a U.S. person where that person is a target, I support, believe in and would strongly endorse that we have a warrant. That warrant is

given to us by a court, and that's not a menial process to go through because it's probable-cause standard. Some would argue, well, you can go really fast because in an emergency you can get just a phone call, but you're still meeting a probable-cause standard. So the director of NSA, me, the attorney general, we're not going to go fast until we have the facts in front of us because it ultimately has to stand the scrutiny of a court.

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

MR. McCONNELL: That's correct.

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

MR. McCONNELL: If you're an American citizen or even a non-citizen in the country, you have the protection of a warrant issued by a court before we can conduct any kind of a surveillance.

Now, sir -- so you're aware. Some will argue that we're targeting overseas and the person overseas called in the United States -- that's where minimization starts.

We can't control what the overseas target does; we have to have a process to deal with that, and that's where minimization was introduced. It's an elegant solution. We have tried every way we can think of to make that different or stronger or more complete, and those who framed this law in '78 and all of us that have looked at it since, we can't find a better process.

SEN. COBURN: But those minimization procedures like Dr. -- like Senator Feinstein suggested have been looked at by the FISA Court.

MR. McCONNELL: They have.

SEN. COBURN: And you are suggesting that you would be happy to have those reviewed, and those probably should be reviewed sequentially and annually.

MR. McCONNELL: By not only the court but by the Congress.

SEN. COBURN: Right.

MR. McCONNELL: And whatever periodicity they would -- they need to review them to be comfortable with doing it the right way.

SEN. COBURN: I have no other questions.

SEN. LEAHY: Thank you very much, Senator Coburn.

Senator Cardin.

SEN. BENJAMIN L. CARDIN (D-MD): Thank you, Mr. Chairman. Admiral McConnell, I very much appreciate your service to our country, and I can tell you that we all agree that we need to make sure that our intelligence community can get the information they need protecting the civil liberties of the people

in our country. We also agree we need to modernize our laws and gather intelligence information.

But let me just suggest that I have confidence in your administration of the agency, but the laws that we create today is going to go well beyond your term in office, so we need to make sure that we have the right laws in place. I agree with Senator Specter's observations that some of the administrative decisions should be placed in statute in order that we have the protection, and I think that's a good suggestion that was made by Senator Specter. I appreciated also your analysis of the law in the 1970s. This is not paranoia. In the '50s and '60s, we had serious problems dealing with the civil liberties of the people in this country, and the FISA Court law was developed in order to provide the right balance. And as you pointed out in your testimony, that you agreed with that law at its time but it needs now to be modernized.

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

Now, you don't need to be a lawyer to know that's a pretty difficult standard for the court to use to set aside the procedures that have been developed. We are talking about the civil liberties of the people in this country. It seems to me that's a pretty tough standard for the entity, the branch of government that's supposed to be our checks and balance -- in order to get involved and suggest changes, they would have to find that your procedures are clearly erroneous. Your comments on that?

MR. McCONNELL: Sir, the target that you're describing is foreign; it's not a U.S. person. So the procedures we're talking about is --

SEN. CARDIN: But it's been pointed out before that in that process, there is very likely at times to be U.S. -- communications with U.S. citizens. So there is the information being gathered potentially involving U.S. citizens.

MR. McCONNELL: The procedures in question you're describing are the procedures to determine foreignness -- that's an odd term, but it's, how do we know that the person being is foreign? So it's -- has a foreign context.

As we discussed with minimization, if you are targeting that foreign person in a foreign country, you can't control who they might call; that's where minimization comes in. If the foreign terrorist calls into the United States, what do you do with that call? Since we can't determine ahead of time who they might call -- some say, well, it's easy, just make it foreign to foreign. You can only target one thing at a time. And while the vast majority of the time it's foreign to foreign, in that isolated instance when it might be foreign to U.S., how do you deal with it? And that's the elegant solution that was captured in 1978, and all I'm arguing is return us to 1978.

We had this same debate and situation in '78. When the means of communication was wireless -- the only thing that has changed that it went from wireless to wire, so that's why we found ourselves in this box.

SEN. CARDIN: I guess my point is this: You make a very persuasive argument that to require an individual application to the FISA Court on a case involving a foreign person would be too onerous and be ineffective in getting the information.

So Congress is looking at saying: Okay, rather than the individual case, take the process that you're using to the FISA Court and have more involvement of the FISA Court on the process. I'm not sure we got it right -- in fact, I don't believe we got it right -- in the last bill we passed as to the appropriate balance between the FISA Court and your work on approving the procedures that are used.

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

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

What I'm worried about is because we've -- we were in a time crunch before, we're in a situation where laws -- words were about to be put in law, which is very difficult to back away from, that would have introduced uncertainty that I feel confident would have inhibited our effectiveness.

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

SEN. CARDIN: That's a fair enough challenge.

I would just submit that we have a couple of months now before the deadline approaches. And it would be useful if we have a meeting of the minds, if that's useful to try to improve the checks and balance(s) through the FISA Court process. Your suggestions or your attorney's suggestions in that would certainly be a good starting point for us in reviewing that, and it would be helpful if we could get that information to our committee.

MR. McCONNELL: All right.

SEN. CARDIN: Thank you, Mr. Chairman.

SEN. LEAHY: Senator Sessions.

SEN. JEFF SESSIONS (R-AL): Thank you.

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

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

MR. McCONNELL: Yes, sir, that's correct.

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

MR. McCONNELL: Yes, sir, I do agree with that.

SEN. SESSIONS: Well, I am then frustrated because it seems to me the tenor and tone of hearing after hearing after hearing since 9/11 have been, that somehow what you're doing is an attempt to constrict the great freedoms that Americans believe in, and we've forgotten the dangers that we face.

And I would just note with regard to 1978, nobody denies that the people in 1978 were striving as best they could to correct some abuses that had occurred. But they created a wall of separation between the CIA/foreign intelligence and domestic intelligence, and the 9/11 commission concluded that was disaster.

MR. McCONNELL: Yes, sir.

SEN. SESSIONS: And we reversed that, clearly, promptly, when we faced to what the good-intentioned people did in 1978. Also in 1978, through good intentions, they prohibited intelligence officers from undertaking operations and informant relationships with people around the world who may have had bad records. Do you remember that?

MR. McCONNELL: Yes, sir, I do.

SEN. SESSIONS: And the intelligence community was concerned about that at the time, but Congress didn't listen, and we did that. And after 9/11, that wonderful idea was examined in the cold light of day and promptly changed and eliminated. So our danger, I would submit to my colleagues, is that, through good intentions, we can create laws that, in fact, inhibit the legitimate ability of this nation to protect itself.

Now, having been through this and having had in 12 years as a United States attorney, I think, one or two wiretaps, I know a little about that. And let me just ask you -- you're not a lawyer, admiral.

MR. McCONNELL: No, sir. (Chuckles.)

SEN. SESSIONS: You're doing pretty well for a non-lawyer, I have to tell you. But when you obtain a wiretap in the United States on an American citizen, it takes a good deal of effort to do that.

But once you obtain the ability through a court order, a great effort, then you -- you don't just -- a person doesn't just talk to himself on a phone; you listen to who the person talks to.

MR. McCONNELL: Yes, sir.

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

MR. McCONNELL: Yes, sir.

SEN. SESSIONS: Isn't that right?

MR. McCONNELL: That's correct.

SEN. SESSIONS: And so if they happen to call not a foreign person, but call somebody in the United States, then that's expected to me from the beginning that they might do that, and you would want to listen to that conversation.

MR. McCONNELL: Yes, sir.

SEN. SESSIONS: I don't see that fundamentally that's any different than the principle I have referred to about a lawful, warranted wiretap here. So you listen to people who call.

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

MR. McCONNELL: Yes, sir.

SEN. SESSIONS: Is that right?

MR. McCONNELL: That's correct.

SEN. SESSIONS: And how do you do that again?

MR. McCONNELL: It's just expunged from the database.

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

MR. McCONNELL: Yes, sir, that'd be -- that's a judgment call. There'd be some potential risk.

SEN. SESSIONS: But as an effort to go -- to avoid criticism from those who always seem to be unhappy with what you're doing, you've gone to the extent that you would minimize that call by removing the name from the system.

MR. McCONNELL: Yes, sir.

SEN. SESSIONS: Now, let me ask you, if a person has been identified to be associated with a terrorist organization, they're somewhere in the mountains of Afghanistan, and they're calling someone in the United States talking about a meal, what kind of television set they have, do you still -- and it seems to be innocent -- do you still minimize that call?

MR. McCONNELL: We would; it would be a judgment call. We'd hope we'd have continuity on the person we're targeting, so if we had some reason to

believe -- and let's suppose that a discussion about a meal could be interpreted about planning for an operation. At that point, one, you would report the information; and two, if that person -- U.S. person in the United States -- you would coordinate with the FBI then to get a warrant against that person to find out if it was, in fact, terrorism related.

SEN. SESSIONS: But you wouldn't have a basis to get a warrant based on what appeared to be an innocent phone call, in fact. And so the only connection you have here is that someone in the United States is talking to a terrorist --

MR. McCONNELL: Yes, sir, that's correct.

SEN. SESSIONS: -- and you're minimizing that unless it appears that conversation had some relationship to what might be an unlawful activity.

With regard to Senator Leahy's comments suggesting that you misstated the impact of this -- the FISA law, I'd like to give you a chance to explain that again.

I thought -- your explanation made a lot of sense to me. Anybody can make a mistake, but I think your testimony was quite accurate, as you understood it. Would you explain that?

MR. McCONNELL: Yes, sir.

I've used some numbers a couple of times. Somebody asked me "What's the significance of this program," and the point I was trying to make, it's probably somewhere in the neighborhood of 50 percent or more of our total collection to understand this threat.

Once you take FISA as a standalone, people have asked me, well, what had happened with the wording of the old law based on subsequent reviews by the FISA Court? And the answer I gave them is we had been reduced by about two-thirds of what our capability was over that period of time. So we were getting into an extremist situation. Known terrorists overseas we weren't able to target without a probable-cause-level warrant.

Probable cause is a hard standard to satisfy, and so it takes time. So working those off, we started in the spring to try to work them off. And in fact, over the summer, we were falling further and further behind because there are lots of potential targets, and a single target -- single human being could use multiple avenues of communication. So you find yourself catching up. That was the first problem.

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

SEN. SESSIONS: Well, just -- and to get a probable cause for a warrant is a -- probably takes a hundred or more pages chock full of facts and figures. It's very difficult to write, and if you're in error the prosecutor -- I mean, the law officer will be accused of perjury. So they have to do it right, and it takes a lot of time.

MR. McCONNELL: Yes, sir. SEN. SESSIONS: Thank you, Mr. Chairman.

SEN. LEAHY: Senator Feingold.

SEN. RUSSELL FEINGOLD (D-WI): Thank you, Mr. Chairman.

Thank you for coming before the committee, Mr. Director.

I'd like to start just a bit by following up on Senator Kennedy's questions about immunity. And with regard to the retroactive immunity you're seeking, how can members of this committee evaluate that request without facts about the alleged conduct in question?

So you should be -- those facts should be available to you.

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

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

SEN. FEINGOLD: You have refused to provide presidential authorizations and DOJ opinions --

MR. McCONNELL: No, sir, I haven't refused.

SEN. FEINGOLD: -- that I think are critical to understand this.

MR. McCONNELL: I haven't refused to provide the committee with anything. I am in a position where I'm attempting to conduct a mission. I have an administration that I work for and I've had a dialogue about how that might play out. As I understand it, there's a negotiation between the chairman and those in the White House about how this might play out. So I've made my recommendations, but I don't control the process.

SEN. FEINGOLD: Well, I think that's critical, and I would say that if --

SEN. LEAHY: Without going into the senator's time, and your recommendation was what?

MR. McCONNELL: We need to provide the appropriate level of insight and information for the committee to get us to the place where we can get the right legislation for this mission going forward.

SEN. FEINGOLD: Does your recommendation include presidential authorizations and DOJ opinions?

MR. McCONNELL: Sir, I don't want to go into that level of specificity.

SEN. FEINGOLD: Well, I would really suggest that if you're serious about this immunity proposal, which you obviously are, you have to make sure that Congress has what it needs to evaluate it. That's just -- that's just a bare minimum for us to be able to do our job. You -- you have a job to do and you're trying to do it well.

MR. McCONNELL: Yes, sir.

SEN. FEINGOLD: We want to be in the same position.

MR. McCONNELL: I understand.

SEN. FEINGOLD: The only way we can be that way is to have the materials so we can understand this.

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

MR. McCONNELL: That was a pretty complex question. In there you said "unlawful." I'm not suggesting anything -- endorsing anything that's unlawful, so --

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

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

SEN. FEINGOLD: You and Mr. Wainstein have stated several times in hearings over the last couple of weeks, and I think you said it again here today, that you would be willing to look at language proposed by members of Congress for changes to the Protect America Act, but that you, of course, want to be careful to ensure that there aren't unintended consequences --

MR. McCONNELL: That's correct.

SEN. FEINGOLD: -- do not result from what may seem like small changes in the language.

I take your point, but the point I want to emphasize here is I think that obligation goes both ways.

Congress has to be careful also not to unintentionally authorize activities that we don't want conducted. And by now I know there's been some back and forth about this. You are very familiar with the controversy surrounding the language in the PAA authorizing acquisition of information, quote, "concerning," unquote, persons outside the United States. Why was this word concerning used, and why should -- (audio break)? (Audio break) -- talking about a proposal. This is the law of the land. And this points up the problem with this rush to judgment that we had in the last-minute push to get this bill passed when you weren't even comfortable with this language.

And I have to say that, you know, we have to be a little worried about this sort of thing because this is the same administration that claimed in one of the most absurd legal arguments I've ever heard that the authorization Congress passed to use military force in Afghanistan after 9/11 somehow allotted to wiretap Americans in the United States without a warrant, and they did so for years in secret. So, you know, when members of the administration say that we should more or less trust them with something like this, which some would argue in favor of this kind of language, members of the public and the Congress have every right to be skeptical, and we have a duty to deal with it. But I do appreciate the fact that you've acknowledged that there are concerns with the word "concerning" and that we have to take it seriously.

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

MR. McCONNELL: I do.

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

MR. McCONNELL: As I tried to explain before, you can only target one thing. And so if the U.S. person in this country -- for whatever reason, terrorists or whatever the issue is -- becomes a target, then you would be required to have a warrant. Now, if you engaged in that process of reverse targeting, where you're targeting someone overseas and your real target's in the United States, that would be a violation of the Fourth Amendment. That's unlawful.

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

MR. McCONNELL: The information is being prepared now. And yes, I can do it with regard to the new authorities.

SEN. FEINGOLD: And when can we receive it?

MR. McCONNELL: I don't know what - I've tasked it. It's -- I'm waiting for response back. I don't know yet. It will -- as soon as I know, I'll be happy to advise you.

SEN. FEINGOLD: Days? Weeks?

MR. McCONNELL: I'd say weeks.

SEN. FEINGOLD: During a hearing of the House Intelligence Committee, you stated that the bulk collection of all communication originating overseas, quote, "would certainly be desirable if it was physically possible to do so,"

unquote, but that bulk collection of communications with Americans is not needed. Is bulk collection of all communications originating overseas, including communications of people in the United States, authorized by the Protect America Act?

MR. McCONNELL: It would be authorized if it were physically possible to do it, but the purpose of the authorization is for foreign intelligence. So when I say -- SEN. FEINGOLD: So there's nothing -- there is no language actually prohibiting this.

MR. McCONNELL: So long as it's foreign, in a foreign country, for foreign intelligence purposes.

SEN. FEINGOLD: Thank you, Mr. Chairman.

SEN. LEAHY: Thank you.

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

MR. McCONNELL: Sir, I don't know what you mean by "taking."

SEN. LEAHY: Well, we take away somebody's rights to have a suit. We do it retroactively. We do it without any compensation. I just throw it out. Your lawyers may want -- don't you try to answer, but it's interesting if we're talking about environmental law; it's terrible, that we would consider this as a taking; but if we want to remove somebody's rights to a suit, it's not.

Senator Whitehouse.

SEN. SHELDON WHITEHOUSE (D-RI): Thank you, Mr. Chairman.

Admiral, good to see you again.

MR. McCONNELL: Thank you, sir.

SEN. WHITEHOUSE: Some of what we're going to discuss will be well-plowed ground between the two of us because we've had these discussions in closed sessions, but I think it's important to go over it again in a public session because it's my very, very strong belief that the problems that we face in adapting the Protect America Act to protect American citizens are very solvable, and had it not been for the atmosphere of stampede that was created in the waning days of the session and we'd had a little bit more time to talk coolly with one another, we could have solved it working off a very sensible template; which is Title 3 surveillance that takes place in the United States right now, such as the senator from Alabama mentioned a moment ago.

In that context, it's my understanding that there are basically two categories of surveillance of Americans that are of concern under the Protect America Act. One is the surveillance of an American when they are abroad, and the second is the surveillance that is incidental to the intercept of a

target abroad when they happen to speak to an American. Can we talk about them in those general two categories?

MR. McCONNELL: Yes, we could, in a foreign context. Of course, if it's in the United States, it's -- (inaudible) -- warrant.

SEN. WHITEHOUSE: (Inaudible) -- that's covered by existing law.

MR. McCONNELL: Right.

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

MR. McCONNELL: That's correct.

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

MR. McCONNELL: You could interpret it that way.

SEN. WHITEHOUSE: And the protection against it being interpreted that way is an executive order that requires the attorney general to assure that the target is an agent of a foreign power, correct?

MR. McCONNELL: That's correct.

SEN. WHITEHOUSE: Now, the domestic model for this kind of surveillance requires, very consistently with the American system of government and the separation of powers, that a court get involved, and that the executive branch -- the FBI, for instance -- doesn't get to make that determination on its own.

MR. McCONNELL: Yes, sir. But you -- what you just shifted to was a domestic situation where you have warrant. And what I would highlight is in the vast majority of the situations that would involve this community, we're targeting a foreigner for which there is no warrant, so it's a little bit --

SEN. WHITEHOUSE: I agree, but I'm talking about where you're targeting an American who happens to be abroad. That's the category we're talking about here.

MR. McCONNELL: Okay.

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

MR. McCONNELL: Sir, that's a possibility, and as we've discussed the last time we talked about this, it sounds reasonable here at the line of scrimmage. But let's see the language and examine it, make sure it says what you want it to say and doesn't impact us in some way that causes a loss of

flexibility. And if given it doesn't have any unintended consequences, I personally would have no objection to that.

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

MR. McCONNELL: I would.

SEN. WHITEHOUSE: Okay.

The other issue is the incidental intercepts. And, as Senator Sessions pointed out, those happen all the time. Like him, I have obtained wiretaps before, both as United States attorney and attorney general. In fact, as attorney general, I had to do it myself, personally, with the presiding judge of the superior court because Rhode Island is careful about letting that authority loose.

When it takes place in a Title III context, the restriction on what is overheard from those incidental interceptions of people who the target calls is protected by minimization procedures, just the same way when somebody calls the target -- when you're targeting somebody overseas and they call an American, that is also protected by minimization procedures. Correct?

MR. McCONNELL: That's correct.

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

MR. McCONNELL: That's my understanding.

SEN. WHITEHOUSE: That doesn't follow into the foreign targeting situation. And so, if we were to make an equivalent role for the FISA Court, to me it would require the FISA Court to do two things: one, approve the minimization procedures themselves -- which, frankly, they do every time they issue a warrant because they write in that order --

MR. McCONNELL: That's correct.

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

MR. McCONNELL: You just introduced a level of complexity and uncertainty that I would say, I'd be happy to look at it. Now, what do I mean by that? In every case where there's Title III, in every case, a court has already agreed in advance that you're going to conduct a surveillance. And there are even -- as I understand it, there are even some requirements for the government to notify the party that you conducted surveillance against in a criminal situation.

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

SEN. WHITEHOUSE: That's not my intention either. My intention simply is to assure that if you got into a situation in which there was a renegade area in the intelligence community someplace, in which they just simply weren't complying with minimization -- we've had unfortunate incidents about the national security letters, and the rules just weren't complied with. It is helpful, I think, and it's salutary, for the executive branch officials discharging a responsibility like that to know that a court can look in. And whether it's the inspector general reporting to the court or whether there's some -- but I do think that it's critical that there be a FISA Court role, just as there would be for incidental intercepts on the U.S. side, to oversee and make sure that the incidental intercepts are being minimized properly in the intelligence context.

MR. MCCONNELL: Yes, sir, and when we discussed this before, the same answer -- happy to sit down, take the language, look at it, have it examined with some time, not like where we were before, so that we really understand, what are the intended and the potentially unintended consequences?

SEN. WHITEHOUSE: Yeah, thank you.

MR. MCCONNELL: And so we both satisfy ourselves that we're protecting Americans and we're not impacting our foreign intelligence mission. And I'd be happy to do that.

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

SEN. LEAHY: Well, the senator from Rhode Island's right. And one of the reasons we're having these hearings now, before -- well in advance of the time when the sunset provision comes is so we can do that. Whereas many of us thought we had worked out that and were quite surprised when apparently at the -- what many of us thought was the last moment, we -- seeing the administration had a different idea, the chairman of the Senate Intelligence Committee has written a significant letter. And I don't know if that letter is classified or not, but I know the senator from Rhode Island has seen it.

Senator Kyl.

SEN. JON KYL (R-AZ): Thank you, Mr. Chairman.

Admiral, you've made the point, I think, very clear that the intelligence collection at issue here is vital to our national security and that Americans' rights are not being violated. But from a lot of the questions, I suspect to the average American this seems very complicated.

And I would like to just have you explain two things for us, using the most direct language you can in a nonclassified context, to explain why this

kind of collection is not suited to the usual court procedure for a criminal suspect like we would see in a TV series, for example, and why it's not constitutionally necessary, in any event.

MR. McCONNELL: Sir, the situation that we find ourselves with is, literally there are billions of transactions. And the targets of foreign surveillance are very dynamic, and they change, and they could change modes of communication and so on.

So for us to have the inherent flexibility that we need to be responsive and to collect the information we need to protect the country, being encumbered by a court process to extend due process rights to a foreigner, a terrorist located overseas, puts us in a situation where we can't be flexible, we can't keep up.

We started this process last winter, and because of the wording in the old law, it was requiring us, because communications had completely flipped from 1978 to the -- until today, whereby international communications were on a wire, fiber-optics, and they happened to flow through the United States -- then we were in a situation to do a foreign target, foreign country; we had to stop and get a warrant.

It is so dynamic that we were losing ground. We had a level of capability. It was reviewed by the court. We started at that level. And subsequent reviews -- not because of the court, because of the wording in the law -- we started reducing our capability. It was reduced in that review period about two-thirds.

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

So I felt a responsibility to identify that as an issue. The law captured it one way in the late '70s, technology changed, and we just need to recognize that and accommodate it to make it technology-neutral. That's the sum and substance what we were attempting to do.

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

And so those are the principles. And, you know, we are where we are with this law that was passed, and we're going to review it again. That's what I'm going to try to -- maintain consistency with regard to our capability so we can indeed protect the country. And all the things that are suggested -- there were seven bills exchanged back and forth, some of them attempting to fix A in fact should have done B or C or D, and that's when I say I'm happy to look at it, but we got to examine it in the cold light of day.

SEN. KYL: Never in the past -- I mean, again, I hate to make it a matter of entertainment, but you see the spy movies and so on, and when we send our spy abroad or James Bond is out looking to collect secrets -- if you're

abroad and you're collecting secrets against an enemy that's abroad, there's never been a requirement for a court warrant, has there?

MR. McCONNELL: No, sir.

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

MR. McCONNELL: No, sir. All that was -- the attempt was to take what was captured in '78 -- which in my view was right -- and make it relevant to 2007.

SEN. KYL: And this is very important information in going after terrorists that we're fighting --

MR. McCONNELL: Sir, it's vital. If we don't have access to this, we are in most cases blind.

SEN. KYL: Right. And when you finally identify an American as somebody that we want to target, then the procedures, the usual due process procedures that we --

MR. McCONNELL: Get a warrant.

SEN. KYL: -- then they apply.

MR. McCONNELL: Yes, sir. SEN. KYL: Now, someone said, well, but if you find that you're beginning to focus in on somebody because he's making quite a few domestic calls, calls that, you know, you can't know when you first look at what he's doing, where those calls are going, but it turns out that some of them start being made domestically -- first of all, might that be important for us to know? And if so, why? And -- well, let me ask that first.

MR. McCONNELL: Well, it could be the most important call we would do in a long period of time, because that may be activating a sleeper cell. So the only way we would know that is when a targeted foreigner activates by calling in, so that was why it would be essential for us.

SEN. KYL: And if you had some kind of arbitrary number that said, well, you have to have a warrant if the person has made more than 15 calls into the United States or something, it'd be pretty obvious what they'd do is simply make 16 calls -- (laughs) -- to a pizza parlor or something and then make another call. In other words --

MR. McCONNELL: Yes, sir.

SEN. KYL: -- if we put statutory limitations that are in statutes and therefore obviously are public, it could be possible for terrorists to get around the intent of what we're trying to accomplish here.

MR. McCONNELL: Yes, sir. It would take away their inherent flexibility. I'd also highlight that in the eyes of the law, a U.S. person could be not only a human being, it could be a corporation.

SEN. KYL: Right.

MR. McCONNELL: So if terrorists are ordering parts or scheduling travel or whatever, that may be of vital interest to us to track the terrorists, not intending that we're tracking a travel organization or an airline or whatever.

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

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

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

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

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

SEN. KYL: In time.

MR. McCONNELL: Yes, sir, in time.

SEN. KYL: Yeah, thank you, Admiral.

SEN. LEAHY: Admiral, are you aware of any time that this administration's asked for a change in the FISA law and it hasn't gotten it?

MR. McCONNELL: I think there was a request, yes, sir, I believe. Some members of this committee introduced legislation, and then it was passed on the House side, but I guess there was no agreement so it didn't pass.

SEN. LEAHY: But then we -- but was that requested by the administration?

MR. McCONNELL: I don't know the origin of the source.

SEN. LEAHY: Just thinking of seven or eight during this administration, it seems we must have been answering some of their questions.

MR. McCONNELL: The language originated on the Hill last year, sir. I've just been advised. Wasn't playing, so I just didn't know.

SEN. LEAHY: Okay. Now, you have reported the use of minimization procedures, and those of us who have been here since the beginning of this are aware of those. But under the Protect America Act, minimized communications are not destroyed; they're maintained in a database. Is that not correct?

MR. McCONNELL: That's not correct, no, sir.

SEN. LEAHY: It's not.

MR. McCONNELL: No. If you minimize, you would take them out of the database. What the -- minimization today is exactly as it was in 1978. That's -- that was the agreement, the process that was agreed to --

SEN. LEAHY: So these minimized communications are not maintained in a database.

MR. McCONNELL: No, sir. If it's in the database and recognized, it would be expunged from the database. Now what you're making reference to is this is the fourth hearing on this subject over this -- since last Tuesday, and in there what I talked -- in a previous hearing, I talked about data that may be collected in a database that you don't know it's there.

SEN. LEAHY: All right.

MR. McCONNELL: You wouldn't know it's there until you had reason to go search it. So it could be there --

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

MR. McCONNELL: It does, if there is -- any time it involves a warrant and a U.S. person, the court would in its ruling have available to it in the context of minimization and --

SEN. LEAHY: Are they shown the minimization procedures the government uses?

MR. McCONNELL: I'm sorry, sir?

SEN. LEAHY: Are they shown the minimization procedures --

MR. McCONNELL: Yes, sir, they are. They are.

SEN. LEAHY: Yup.

I will do a couple of follow-up questions on this for the record, and I hope you and your lawyers look at it very, very carefully. As I said, I'm not trying to play "gotcha" and that there are answers in here where, upon reflection, you think they should have been different. You know, plenty of times we do that --

MR. McCONNELL: I appreciate that, Mr. Chairman.

SEN. LEAHY: You've identified as one of your highest priorities getting the retroactive immunity -- and we've touched on this; several of us have -- to communication companies that may have broken the law in helping to carry out the government's secret surveillance program after 9/11.

As you may know, the state of Vermont, along with a number of other states, is seeking to investigate some telecommunication carriers for disclosing consumer information to the NSA in that program. There's a lawsuit, I believe, in the 9th Circuit that would be dismissed if the carriers got immunity. That's why I asked the question about taking. Now, this committee has issued subpoenas, voted for by both Democrats and Republicans, seeking information on this. We've received no documents, no information about the legal justification for the warrantless surveillance program. We're in the dark about what the legal justification was, what communications took place between the administration and the communication companies to secure private sector cooperation for the program; for two years have been seeking the legal justification and the analysis, what the administration relied on to conduct the president's program of warrantless surveillance. We are, however, asked to pass laws to immunize everybody and to wipe out of court any cases. And basically we're asked to do it on a total "trust me" basis. "We won't tell you what we did or what we based it on or why, but please pass the law saying that you've made a studied conclusion that everything we did was okay and let's immunize us." It's -- I'm not sure, if you were presented with something like that, you would be too eager to accept that.

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

MR. McCONNELL: And, sir, that's a call the White House will have to make. My personal philosophy in how to conduct this business is oversight's a good thing. It keeps the system honest. And so engaging with the Congress provides an appropriate level of information for the oversight process is what we should do.

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

SEN. LEAHY: No. I'm saying as DNI, just simply as DNI -- obviously the judgment call is going to be made by the administration -- but do you have -- as DNI, do you have any objection to these legal memoranda being shared -- these historical legal memoranda being shared with this committee?

MR. McCONNELL: Sir, my history on this starts in January when I was nominated and February when I was confirmed. What I'm trying to do in my role --

SEN. LEAHY: But obviously you've seen the historical and legal --

MR. McCONNELL: I have not. I have not. What I've attempted to do here is to take what -- where we are today and put it wholly under the law in the FISA process for how we conduct our business, all of it. There's nothing extreme or -- so anything that we do in the nature of the business we're talking about would make it --

SEN. LEAHY: But, Admiral, you're up here lobbying to have us wipe out these courts by -- wipe out these cases retroactively by legislation.

MR. McCONNELL: Sir, I would --

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

MR. McCONNELL: No, sir, it isn't. First of all, I object to the word "lobbying"; I'm here because you invited me here. And I'm testifying, not "lobbying." SEN. LEAHY: I'm thinking of some of the -- during -- I'm going back to July and August in some of your meetings. You call it whatever you want. You were advocating for retroactive legislation.

MR. McCONNELL: I am -- I have a responsibility, as the leader of the nation's intelligence community, to make recommendations to this body and to the administration about what it is that we need to do our job, and that's how I saw my role, and that's what I hope to -- in the final analysis, when we look back, that's what I was doing.

SEN. LEAHY: Are you doing -- are you conducting -- if you want to answer this -- under the PA or otherwise, are you conducting physical searches of homes or business of Americans or Americans' mail without a warrant?

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

SEN. LEAHY: But you're not?

MR. McCONNELL: No, I'm not.

SEN. LEAHY: Senator Specter.

SEN. SPECTER: Thank you, Mr. Chairman.

Just a couple of questions, because we have another panel waiting to be heard. But I questioned you on the first round -- I brought up the issue of the targeting of U.S. persons overseas and noted that there is an executive order which requires the attorney general to certify that there is probable cause. My own view is that there ought to be that determination made by the FISA Court, and in a response to the question from Senator Hatch, you said there are only about 50 to 55 of those a year, so it wouldn't be a great administrative burden.

Would you concur or, perhaps better stated, have any objection to the next version of the statute to give the FISA Court the authority to authorize targeting U.S. persons overseas?

MR. McCONNELL: Sir, as I indicated earlier, I would have no personal objection. What we'd have to do is look at the language to examine any potential unintended consequences. The difference would be the authority for the warrant going from the attorney general into the FISA Court. So that seems to me, on the face of it, to be a manageable situation.

There were -- there are reasons that we could go into in a closed session that it was set up the way it is, and I'd be happy to share that with you. But we must examine that in a closed session, make sure it doesn't have unintended consequences, and I'd be happy to say let's examine it.

SEN. SPECTER: Are you are saying that there are reasons to invest it in the attorney general, the determination of probable cause, instead of the FISA Court? And when probable cause is established, that's the traditional basis for the issuance of a warrant.

MR. McCONNELL: Yes, sir.

Let me separate "U.S. citizen" from "U.S. person." And some -- in "U.S. citizen," it's easy. "U.S. person," it may present a situation that we'd just need to make you aware of the full range of potential impact.

SEN. SPECTER: But it's "U.S. person" who has to -- where you have to have a warrant for targeting in the United States.

MR. McCONNELL: That's correct. Yes, sir.

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

MR. McCONNELL: I was trying to highlight the -- in my view, a U.S. citizen shouldn't expect to give up their rights, regardless of where they're located. So it's a higher standard for "U.S. citizen" as opposed to "U.S. person." A U.S. person can be a foreigner. It could even be a terrorist that was located in the United States -- say, a foreigner here, a green card. In the legal context, you could consider that person a U.S. person even though they travel back overseas. So I'm just trying to say there's an issue in there we need to examine.

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

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

MR. McCONNELL: Yes, sir. When I -- and you said "person." I'd just highlight -- make sure it's foreign person, located overseas. That's the part that they --

SEN. SPECTER: Foreign person located overseas.

MR. McCONNELL: Foreign person, yes, sir.

SEN. SPECTER: Okay. Now, you need the flexibility to do that without prior approval by the FISA Court because of the numbers involved?

MR. McCONNELL: Yes, sir. It's a very dynamic situation.

SEN. SPECTER: Dynamic? You mean large? Large numbers?

MR. McCONNELL: Large. Huge. Huge, yes, sir.

SEN. SPECTER: Dynamic meaning --

MR. McCONNELL: Fast-changing --

SEN. SPECTER: -- too many to do, you say?

MR. McCONNELL: Yes, sir.

SEN. SPECTER: Well, explain why that -- why that is, why --

MR. McCONNELL: The --

SEN. SPECTER: Let me finish the question. -- why you can't handle that administratively to submit those applications to the FISA Court for -- with a statement of probable cause.

MR. McCONNELL: Well, first of all, it's extending probable cause standard and Fourth Amendment protection to a foreigner overseas, so my argument would be, to maintain the flexibility of our community to do our mission, why would you insert that as a standard, because it's an additional burden on the community to be flexible?

Now --

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

MR. McCONNELL: Yes, sir. It is unreasonable on the face of it, and it precludes us from being effective in --

SEN. SPECTER: Okay. Now, the question is why. Just as a result of the sheer numbers?

MR. McCONNELL: Numbers and the dynamic nature of it. Most of our conversation today --

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

MR. McCONNELL: Fast-paced. Rapidly changing.

SEN. SPECTER: Okay.

MR. McCONNELL: And we've all -- most of our discussions have been around terrorists, which sound like, well, that's a reasonable number of people. But the foreign intelligence mission of the community is foreign, so by definition, it's anything that's not American. And when we've taken great pains in a number of cases to prioritize who we target and so on, we inevitably get it wrong. Previous administration, we did a tiering mechanism, like 1 through 5; 5 was absolute targets, got to cover them, got to be very exhaustive in our coverage.

As it turned out, where U.S. forces were asked to engage or in some way be committed, it was almost all in the tiered areas that we weren't covering. And examples include Haiti and Somalia and even as far back as Panama. It's

those situations that pop up which you have to be responsive and dynamic to respond to so you understand who the threats are, how they're changing, what are the intentions, what are the weapon systems, how might they engage, what might cause them to back down.

All that's a very dynamic --

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

MR. McCONNELL: Yes, sir.

SEN. SPECTER: Have you gone back to the FISA Court to go through the procedures which you're now using and targeting foreign persons overseas?

MR. McCONNELL: Yes, sir, we've submitted all the procedures to the court, and they're reviewing them now.

SEN. SPECTER: They're reviewing them?

MR. McCONNELL: Yes, sir.

SEN. SPECTER: Now, would it be too burdensome to ask you to submit those procedures to the court every three months?

MR. McCONNELL: That wouldn't change but that would not be a great burden, no, sir.

SEN. SPECTER: Okay.

MR. McCONNELL: The only thing I want to highlight is if I'm in a position where the court has to rule on something before I can conduct a mission, we could never keep up. It's not -- it can't turn fast enough to allow us the flexibility.

SEN. SPECTER: Well, we're not -- my suggestion would not be to deal with specific warrants, where you'd have to go back, but only the procedure.

MR. McCONNELL: Yes, sir.

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

MR. McCONNELL: Sir, I would be -- I would object to that. Because in my view, it would now start to insert into the process an evaluation by the court, for which it's not trained or prepared, with regard to the effectiveness of the foreign intelligence mission. Let me use a couple of examples.

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

MR. McCONNELL: The purpose in my view of targeting a U.S. person in the United States is to ensure that we have adequate protection. If it's a U.S. person in the United States, they will examine -- first of all, the numbers are

small, very small. They would have the facts of the situation. They could make a judgment and they could do enough research to make an informed judgment.

If you're talking about thousands or tens of thousands or hundreds of thousands of things that are transpiring in a foreign context, my view is that they just couldn't keep up with that process. There are 11 judges. One sits at a time. And this community is made up of tens of thousands of people that are engaged in a very dynamic process, issuing lots of reports and lots of coordination and lots of cross-cueing.

So something that would seem relatively innocuous on the face of it might turn out to be the most important thing we're chasing -- example: movement of nuclear material on a foreign-flagged ship of convenience that's moving from the Pacific into the Indian Ocean. Now, we might not even know that ship's underway. But if at some moment, there's some clue, we've got to be very responsive in how we would try to track back. Where does it originate? What might it have onboard? Where is it going? Who are the players? And so on.

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

SEN. SPECTER: I get your point, Director McConnell. I'm over time, but I want -- this is important and I want to finish it.

MR. McCONNELL: Sir.

SEN. SPECTER: I get your point on the dynamism of being able to act without getting court approval, but I'm on a very different point. I'm on the point of going back for renewal, saying three months as to procedures, and at that time saying to the court we want to continue this under these procedures and this is what we've accomplished, because even -- we're not telling you you can't do it, but we want to evaluate it. And you are reaching some U.S. persons overseas, and we have elaborate minimization, and it seems to me that there is a good basis for having the court take a look at what you've done to see that the intrusiveness, even though there are a lot of foreign people involved, but there are some U.S. people involved, as to whether it's worth the candle.

MR. MCCORMACK: Sir, what -- the reason I would object to it is at the 99.999 percent level it's totally foreign, and so by having the court make that judgment, you're introducing a level of ambiguity and uncertainty that I don't know how it would come out.

So now, let's go back to the U.S. persons situation. In that case, if the court chooses to look at it, post -- they've issued a warrant, ex post facto they want to review -- or as was suggested by Senator Whitehouse, they look at minimization after the fact -- that's more of a manageable problem. But to have the court in the position of saying what you've collected is or is not sufficient intelligence value, my view is that's not the appropriate role for the court.

My worry is a level of uncertainty and ambiguity that I don't know how it'll come out. We do the mission for foreign intelligence.

There are oversight committees on the Hill that look at that, can evaluate it in any cross-cut or any dimension. And we're responsive to the administration who's given us these targets for intelligence collection purposes.

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

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

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

MR. MCCONNELL: Yes, sir, will do, thank you.

SEN. LEAHY: I'm easily reachable.

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

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

END.