

PATRICK J. LEAHY, VERMONT, CHAIRMAN

EDWARD M. KENNEDY, MASSACHUSETTS  
JOSEPH R. BIDEN, JR., DELAWARE  
HERB KOHL, WISCONSIN  
DIANNE FEINSTEIN, CALIFORNIA  
RUSSELL D. FEINGOLD, WISCONSIN  
CHARLES E. SCHUMER, NEW YORK  
RICHARD J. DURBIN, ILLINOIS  
BENJAMIN L. CARDIN, MARYLAND  
SHELDON WHITEHOUSE, RHODE ISLAND

ARLEN SPECTER, PENNSYLVANIA  
ORRIN G. HATCH, UTAH  
CHARLES E. GRASSLEY, IOWA  
JON KYL, ARIZONA  
JEFF SESSIONS, ALABAMA  
LINDSEY O. GRAHAM, SOUTH CAROLINA  
JOHN CORNYN, TEXAS  
SAM BROWNBACK, KANSAS  
TOM COBURN, OKLAHOMA

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

## United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

October 25, 2007

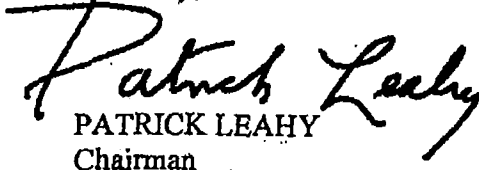
Bryan A. Benczkowski  
Principle Deputy Assistant Attorney General  
Office of Legislative Affairs  
U.S. Department of Justice  
950 Pennsylvania Avenue, N.W.  
Room 1601  
Washington, DC 20530

Dear Mr. Benczkowski:

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

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

Sincerely,

  
PATRICK LEAHY  
Chairman

OLA-93A

Ahmad, Usman

From: Tracci, Robert N  
 Sent: Thursday, October 25, 2007 1:33 PM  
 To: Wainstein, Kenneth (NSD); Benczkowski, Brian A (OLA); Gerry, Brett (OLP); Tracci, Robert N; Demers, John (NSD); Olsen, Matthew  
 Subject: FW: Witness list for hearing on Wednesday, October 31 at 10:00 a.m.  
 Attachments: 07-10-31 FISA Hearing - Witness List.doc

From: Rossi, Nick (Judiciary-Rep)  
 Sent: Thursday, October 25, 2007 1:30 PM  
 To: Tracci, Robert N;  
 Subject: FW: Witness list for hearing on Wednesday, October 31 at 10:00 a.m.

We are waiting for confirmation on our witness, so this will be updated shortly.

From: Price, Jennifer (Judiciary-Dem) [mailto:Jennifer\_Price@judiciary-dem.senate.gov]  
 Sent: Thursday, October 25, 2007 1:22 PM  
 To: All Judiciary Users; Alexander, Elizabeth (Biden); Carle, David (Leahy); Cota, Greg (Leahy); Galyean, James (L. Graham); Ginsberg, Daniel (Leahy); Kolenc, Michael (Durbín); Kuhn, Walt (L. Graham); Nuebel, Kathy (Grassley); Orloff, Nancy (Biden); Pagano, Ed (Leahy); Sandgren, Matthew (Hatch); Saunders, Chris (Leahy); Tardibono, Timothy (Coburn); Upton, Marianne (Appropriations); Branca, Arlene (Kohl); Dowd, John (Leahy); Watts, Nick (Kennedy); Hinck, Kaaren (Whitehouse); Kidera, Daniel (Schumer); Lapla, Joe (Dem-Secretary); McDonald, Kevin (Leahy); Sebern, Will (Feingold); Smith, Michele (Biden); Yamada, Debbie (Cardin); Arif, Samir (Brownback); Edwards, Lauren (L. Graham); Hollis, Kate (Sessions); Montoya, Ruth (Hatch); Moore, Megan (Cornyn); Pepper, Catherine (Cornyn); Plakoudas, Maria (Specter); Shadegg, Courtney (Coburn); Shimp, Leah (Grassley); Stewart, Christine (Cornyn); Pollack, Lizabeth (Feinstein); McInerney, Erin (Kyl); Prendergast, Katie (Kyl); Lisa Dennis; Dean, Ken (Secretary); Brown, Elizabeth (Secretary); Devennie, Brandon (Secretary)  
 Subject: Witness list for hearing on Wednesday, October 31 at 10:00 a.m.

Witness List

Hearing before the  
Senate Judiciary Committee

on

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

Wednesday, October 31, 2007  
Dirksen Senate Office Building Room 226  
10:00 a.m.

Panel I:

**OLA-94**

**Kenneth L. Wainstein  
Assistant Attorney General  
National Security Division  
U.S. Department of Justice**

**Panel II:**

**Edward Black  
President and CEO  
Computer & Communications Industry Association  
Washington, DC**

**Morton H. Halperin  
Director of U.S. Advocacy  
Open Society Institute  
Washington, DC**

Witness List

Hearing before the  
Senate Judiciary Committee

on

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

Wednesday, October 31, 2007  
Dirksen Senate Office Building Room 226  
10:00 a.m.

**Panel I:**

**Kenneth L. Wainstein  
Assistant Attorney General  
National Security Division  
U.S. Department of Justice**

**Panel II:**

**Edward Black  
President and CEO  
Computer & Communications Industry Association  
Washington, DC**

**Morton H. Halperin  
Director of U.S. Advocacy  
Open Society Institute  
Washington, DC**

JOHN CONYERS, JR., Michigan  
CHAIRMAN

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

12/14/07  
MH

LAMAR S. SMITH, Texas  
RANKING MINORITY MEMBER

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

ONE HUNDRED TENTH CONGRESS

# Congress of the United States

## House of Representatives

COMMITTEE ON THE JUDICIARY

2138 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6216

(202) 225-3951

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

October 9, 2007

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

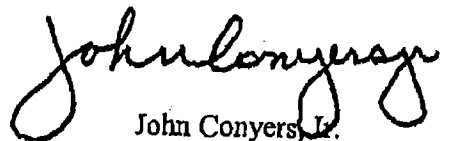
Dear Mr. Wainstein:

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

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

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

Sincerely,



John Conyers, Jr.  
Chairman

cc: Hon. Lamar S. Smith

OLA-98A

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

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

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

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

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

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

**Minimization (Wainstein and McConnell)**

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

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

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

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

8. Does Section 105(B) permit the President to compel communications carriers to conduct domestic wiretaps so long as "a significant purpose" is to obtain foreign intelligence information concerning persons outside the United States?
9. If an individual in the United States is suspected of working in collusion with persons outside the United States – such that an investigation of one is in effect the investigation of the other – under what circumstances, generally, would you use criminal or other FISA wiretaps, and under what circumstances would you use 105(B) authority? Please explain.

---

10. Assuming for a moment that a member of Congress is going to meet with a high-ranking official from Syria, does Section 105(B) permit the wiretapping of that Member's office phone on the grounds that it would produce "foreign intelligence information ... concerning persons reasonably believed to be outside the United States?" Please explain.
11. Does Section 105(B) permit searching stored emails of a Member of Congress who is planning to meet with Iraqi officials? Please explain.

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

**Telecommunications Carriers Immunity Questions (Wainstein and McConnell)**

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



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

Scope of Authority under the PAA (Wainstein and McConnell)

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

cannot instantaneously determine the location of each party.

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

**Metadata Collection** (Wainstein and McConnell)

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

**FISA Exclusivity** (Wainstein only)

27. Does the United States, through its Justice Department, agree that FISA is the law of the land, and that foreign intelligence surveillance must occur within that law? If not, why not?

---

28. Is the President free to disregard any provisions of FISA with which he disagrees? If so, please explain.
29. To your knowledge, since January of 2007, when the Attorney General stated that the TSP was brought within FISA, has all foreign intelligence electronic surveillance occurred consistent with FISA – both prior to and subsequent to the August amendments? Since that time have any electronic surveillance programs been conducted outside the authority of the Foreign Intelligence Surveillance Act as amended by the Protect America Act?

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

**The Federal Bureau of Investigation (Wainstein only)**

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

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

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

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

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

German plot (McConnell only)

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

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

US persons "targeted" for surveillance (McConnell only)

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

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

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

**Declassification of Information (McConnell only)**

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

**Concerns About the House Bill (McConnell only)**

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

**Previous Problems Concerning Warrantless Surveillance and Minimization (McConnell only)**

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

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

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

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

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

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



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

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

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

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

## FISA Questions

### *General Questions*

1. What are the consequences if the Congress does not reauthorize the Protect America Act?
2. Critics of the Protect America Act have suggested that it was passed in the dead of night, without sufficient consideration by Congress. When did the Administration propose legislation to modernize FISA and how many hearings were held on that topic prior to the vote on the Protect America Act? And how many further hearings have been held in the two months since we passed that Act?
3. Some argued that if a terrorist overseas happens to call into the United States, our intelligence agencies should have to go to the FISA Court to intercept that call. Why is this not a workable approach? What about a provision that requires the Intelligence Community to go to the FISA Court for authorization to collect a terrorist's calls if he calls into the United States more than a handful of times. Is that a workable approach?
4. Is it true that under the Protect America Act, as well as under the legislation reported out of the Senate Select Committee on Intelligence, all communications obtained are subject to minimization procedures just like communications obtained under FISA previously? Haven't those minimization procedures worked to protect the privacy of United States persons for the nearly 30 years they have been in place?

### *Senate and House Proposals*

5. Does the Administration have any major concerns with the legislation recently reported out of the Senate Select Committee on Intelligence?
6. How does the legislation reported out of the Senate Select Committee on Intelligence compare to the RESTORE Act that was scheduled to be voted on in the House floor a few weeks ago?
7. It is my understanding that the RESTORE Act would require us to continue to obtain individual court approval to target persons overseas with respect to certain categories of intelligence. Isn't this a step backwards from the Protect America Act?
8. Both the Senate Intelligence Committee bill and the RESTORE Act contain sunset provisions. Haven't we given these questions more than enough consideration to put these new authorities on permanent footing, so that our intelligence professionals will have the certainty they need going forward?

OLP-2A

9. The *Washington Post* described an amendment proposed by Senator Wyden, which would require new court approval of efforts to surveil U.S. persons overseas, as an "unnecessary and potentially disruptive precedent." Do you agree? My understanding is that this amendment would impose requirements in the intelligence context that go beyond what we require in the criminal context for physical search warrants overseas. Is that correct?
10. Hasn't the existing process of surveilling U.S. persons overseas – which requires an individualized determination of probable cause by the Attorney General before surveillance can begin – served us well for decades? Senator Bond and three other Senators (including Senator Hatch) on the Intelligence Committee said in their report that this authority has "worked well" – why would we change it, when the very purpose of this legislation is to get the FISA Court out of the business of approving surveillance on overseas targets?

#### *Immunity*

11. Isn't it true that electronic surveillance for law enforcement and foreign intelligence purposes depends in great part on the assistance of private electronic communications service providers? What message does it send to companies if we do not protect them when they agree to help us?
12. Do you think that private electronic communications service providers are less likely to assist the government with its lawful surveillance activities if they are subject to potentially massive lawsuits based on allegations that they assisted the government?
13. Shouldn't private electronic communications service providers be entitled to rely, in good faith, on the government's representation that a particular intelligence activity was authorized by the President and was lawful?
14. Isn't it simply unfair to permit these companies – who are alleged merely to have done their patriotic duty and assisted the government in the aftermath of the horrific terrorist attacks of September 11, 2001 – to be subject to lawsuits brought by trial lawyers from across the nation?
15. Where a person has provided assistance to the Government pursuant to a written request or order, but it would harm the national security for the request for assistance to be disclosed, doesn't it make sense to create a procedure whereby cases challenging such assistance are dismissed without harming national security?

## The Need for Permanent FISA Modernization

### **Changes in Communications Technology Have Drastically Expanded the Scope of FISA**

- Congress enacted FISA in 1978 to regulate the use of electronic surveillance in the United States for foreign intelligence purposes.
  - Judicial review under FISA was designed to apply primarily to surveillance activities within the United States—where privacy interests are critically at stake—and not to overseas surveillance against foreign intelligence targets—where privacy interests are minimal or non-existent.
- However, as a result of changes in telecommunications technology since 1978, the scope of activities covered by FISA expanded to cover a wide range of intelligence activities that Congress intended to exclude in 1978.
  - This unintended expansion has hampered our intelligence capabilities and caused us to expend resources on obtaining court approval to conduct intelligence activities directed at foreign persons overseas.
- For example, prior to the passage of the Protect America Act of 2007, the Government often needed to obtain a court order before intelligence collection could begin against a target located overseas.
  - As a result, considerable resources of the Executive Branch and the FISA Court were being used to obtain court orders to monitor the communications of terrorist suspects and others abroad.
    - In essence, we effectively granted constitutional protection to foreign terrorists suspects overseas.
  - Moreover, this requirement sometimes slowed, and may have blocked, the Government's efforts to conduct surveillance that was potentially vital to the national security.
  - This expansion of FISA also diverted resources that would be better spent on protecting the privacy interests of United States persons here.

### **The Protect America Act Was a Step in the Right Direction**

- The Protect America Act updated the definition of “electronic surveillance” to exclude surveillance directed at persons reasonably believed to be outside the United States.
  - The Protect America Act represented the right solution—allowing our intelligence agencies to surveil foreign intelligence targets located outside

the United States without prior court approval.

- The benefits provided by the Protect America Act have demonstrated the critical need to reauthorize the Act and to make its core authorities permanent.
  - Prior to the passage of the Protect America Act, the Director of National Intelligence testified that the Intelligence Community was unable to obtain the information that it needed to collect in a timely manner to protect the United States.
  - The Protect America Act has allowed us temporarily to close intelligence gaps that were caused by FISA's outdated provisions.
  - If we are to stay a step ahead of terrorists who want to attack the United States, Congress should make the core provisions of the PAA permanent to ensure that these intelligence gaps must remain closed.

Summary Points: SSCI Bill ("The FISA Amendments Act of 2007")

- The Senate Intelligence Committee bill, which was voted out of Committee with a 13-2 vote, contains many good provisions that would strengthen our national security. For instance:
  - *Collection authority.* Like the Protect America Act, the bill would allow our intelligence professionals to continue collecting foreign intelligence against foreign targets located outside the United States without obtaining prior court approval. Instead, the FISA Court would review after-the-fact the procedures that the government uses to determine that targets are located outside the United States, and the minimization procedures governing the use and retention of U.S. persons information.
  - *Automatic Stay Pending Appeal.* In the event the FISA Court fails to approve these procedures, the acquisition may continue pending any appeal to the Foreign Intelligence Surveillance Court of Review. This is an important provision that is not contained in the House's RESTORE Act, and which is necessary to ensure that we do not go "dark" on overseas targets while legal issues are being considered on appeal.
  - *Retroactive Liability Protection.* The bill affords immunity from private lawsuits for electronic communications service providers who are alleged to have assisted the Government in the aftermath of the September 11<sup>th</sup> attacks, if the Attorney General certifies to the Court that the alleged assistance either (1) was conducted at the request of the Government and described in a written directive indicating that the activity was authorized by the President and determined to be lawful; or (2) did not occur. This is a critically important provision, both because those who supported us in the wake of the September 11 attacks deserve our support, and because the future cooperation of companies in our intelligence efforts is critical to the national security.
  - *Streamlining FISA Reforms.* The bill contains a number of additional amendments to FISA, some of which were drawn from the Administration's April proposal. In particular, the bill adopts elements of the Administration's proposal that would streamline the FISA application process and extend the period of emergency authorizations.
- While the Senate Intelligence Committee bill contains many positive provisions, there are also provisions that are of concern.
  - *Overseas Collection Targeting U.S. Persons.* The "Wyden Amendment" would place the FISA Court in the unprecedented role of approving purely overseas intelligence activities. This could have adverse operational consequences.

OLP-2C

- *Sunset.* The bill would sunset in six years. While this is far preferable to the short sunset in the RESTORE Act, but the vital authorities to surveil overseas targets should be put on a permanent footing, to give the Intelligence Community the tools it needs.
  
- *Burdensome Oversight.* The Act requires, among other things, an annual review to determine “the number of persons located in the United States whose communications were reviewed.” Given the fragmentary nature of foreign intelligence collection and the limited amount of information available concerning any specific intercepted communication, it may well be impossible for intelligence agencies to comply with this requirement.

## Problems with the Leahy Substitute

### Background

- Last month, the Senate Intelligence Committee introduced a consensus, bipartisan bill that would establish a solid, long-term foundation for our intelligence community's efforts to target terrorists and other foreign intelligence targets located overseas. While the bill was not perfect, it contained many important provisions, and was developed through a thoughtful, bipartisan process that included outreach to the Administration for assistance on key provisions.
- The bill was reported from the Senate Intelligence Committee by a 13-2 vote, including votes from two Democratic members who also sit on the Judiciary Committee.
- Just hours before the Senate Judiciary Committee mark-up on this bill, Senator Leahy introduced a complete substitute to Title I of the Senate Intelligence Committee's proposal. This substitute was offered without consultation with any of the FISA experts in the intelligence community or at the Justice Department, and as of now does not enjoy the same bipartisan support as the Senate Intelligence Committee bill.
- The Leahy substitute would make a number of changes that would constitute significant steps backwards from the sound, bipartisan product that came out of extensive deliberation in the Intelligence Committee.

### Specific Problems

- The Leahy substitute (p. 34, l. 11- p. 36, l. 2) contains an amendment to the "exclusive means" provision of FISA that could have radical and adverse effects on our ability to conduct national security investigations and overseas intelligence operations.
  - The Leahy exclusivity provision is unnecessary. The Senate Intelligence Committee bill already has an exclusive means provision.
  - As drafted, the Leahy provision could eliminate the Government's ability to use some common criminal investigative tools in international terrorism or espionage investigations. These include:
    - Title III Criminal Wiretaps.
    - Criminal Pen Registers and Trap and Trace Devices.
    - Search Warrants.
    - Grand Jury Subpoenas.
  - It would eliminate the Government's ability to use certain investigative tools created for national security investigations, like National Security Letters, to collect communications information.

**OLP-5A**



- It could eliminate the Government's ability to use other investigative tools—including possibly court orders authorizing the access of stored communications—in certain national security investigations.
  - This provision could also disrupt highly classified intelligence activities and could harm the national security. Among other things, ambiguities in critical terms and formulations in the provision—including the term “communications information” (a term that is not defined in FISA) and the introduction of the concept of targeting communications (as opposed to persons)—could lead the statute to bar or require court approval for overseas intelligence activities that may involve merely the incidental collection of U.S. person information.
  - The amendment to the section 2511(2)(a)(ii) certification provision contains ambiguities that could harm the Government's ability to obtain the assistance of private partners.
  - The part of the provision purporting to require a future Congress to provide specific statutory authority for surveillance would complicate Congress's drafting, in an emergency situation, of a law to authorize the immediate collection of communications in the aftermath of an attack or in response to a grave threat to the national security. It is unwise to tie the hands of a future Congress in this manner.
- The Leahy substitute would delete an important provision in the bipartisan Intelligence Committee bill (p. 21, ll. 5-13) ensuring that our intelligence professionals can continue to collect intelligence from overseas terrorists and other foreign intelligence targets during the pendency of an appeal of a decision of the FISA court. Without that provision, whole categories of surveillances directed outside the United States could be derailed based on a single judge's opinion before review by the FISA Court of Review.
  - The Leahy substitute (p. 23, l. 14 – p. 24, l. 25) 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. By requiring analysts to go back to databases and pull out the 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. This requirement creates a super-exclusionary rule in the context of foreign intelligence surveillance and is at odds with the 9-11 Commission's mandate to the intelligence community to find and link the disparate pieces of foreign intelligence information—to connect the dots.
  - The Leahy substitute (p. 26, l. 6 – p. 26, l. 19) would allow the Court to review compliance with minimization procedures that are used on a programmatic basis for the acquisition of foreign intelligence information only from individuals outside the United States.

- This proposal could place the FISA court in a position where it would be obligated to 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 here, where the court's role is in approving generally applicable procedures rather than individual surveillances.
  - Unlike in the FISA court's traditional role of approving and disapproving specific applications, this authority could extend to and affect all surveillance carried out under a particular set of targeting or minimization procedures.
- The Leahy substitute would strike a provision from the bipartisan Senate Intelligence Committee bill (p. 31, ll. 20-21) that would allow the second highest-ranking FBI official to certify applications for electronic surveillance. Today, the only FBI official who can certify FISA applications is the Director, a restriction that can delay the initiation of surveillance when the Director travels or is otherwise unavailable. It is unclear why this provision from the Intelligence Committee bill, which will enhance the efficiency of the FISA process while ensuring high-level accountability, would be objectionable.
  - In addition to these steps backwards from the Intelligence Committee bill, the Leahy substitute fails adequately to address those few provisions in the Senate Intelligence Committee with which the Administration has concerns—concerns that were publicly articulated by the Administration to the Senate Judiciary Committee.
    - The substitute fails to make needed improvements to the “Wyden Amendment” to the Senate Intelligence Committee bill, which would require for the first time that a court order be obtained to surveil U.S. persons abroad. In addition to being problematic in its own right and imposing burdens on foreign intelligence collection abroad that do not exist with respect to collection for law enforcement purposes, the provision continues to have serious technical problems.
      - As drafted, the provision would not allow for the surveillance, even with a court finding, of certain critical foreign intelligence targets. The provision incorporates a definition of “agent of a foreign power” that was designed in FISA for use in the context of surveillance primarily in the United States and is thus focused on conduct here. It is too restrictive and does not make sense to use this definition in the context of surveillance conducted abroad of persons abroad.
      - The provision would also inexplicably allow emergency surveillance *outside* the United States for significantly less time than the bipartisan Senate Intelligence Committee bill had authorized for surveillance *inside* the United States.

- The substitute maintains a six year sunset, which the Administration opposes. Indeed, several Democrat members on the Judiciary Committee have indicated that they may propose amendments to the bill that would shorten the sunset, leaving the intelligence community subject to an uncertain framework for collecting intelligence on overseas targets.
  - Any sunset introduces a significant level of uncertainty as to the rules employed by our intelligence professionals and followed by private partners.
  - 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.
  - The intelligence community operates much more effectively when the rules governing our intelligence professionals' ability to track our enemies are established and are not constantly changing. Stability of law allows the intelligence community to invest resources appropriately.
  
- The substitute fails to make needed amendments to a reporting requirement that poses serious operational difficulties for the intelligence community. The Intelligence Committee bill (p. 25, l. 11-13) contains a requirement that the intelligence analysts count "the number of persons located in the United States whose communications were reviewed." This provision might well be impossible to implement. In addition, it does not reflect the way in which intelligence analysis is conducted—for instance, once an analyst determines that a communication is not relevant, he moves on to the next piece of information; he does not analyze the irrelevant communication to determine the location of the persons who were parties to it. To require analysts to do so would not only waste resources but would pose a needless intrusion on privacy.

**The SSCI Bill Represents a Sound Bipartisan Agreement Developed after Careful Consideration, with Full Information, and with Full Understanding of its Impact on our Abilities to Keep America Safe**

- The Senate Select Committee on Intelligence has carefully considered the issues surrounding FISA reform.
  - As the Committee stated, it intended to draft a “bipartisan proposal to replace the [Protect America Act] that would authorize the acquisition of foreign intelligence information in light of the advances in technology since 1978 with improved protections for the privacy interests of Americans whose communications might be targeted or incidentally collected.”
  - The SSCI held seven hearings in 2007 dedicated to FISA modernization and related oversight activities. Witnesses before the committee included a broad range of individuals from the public and private sectors.
  - The SSCI focused on finding the right balance between protecting the country and our civil liberties—with full awareness as to the threats that we face and the potential impact of activities that could be authorized.
  - As noted in the S.2248 Conference Report, the Committee “propounded and received answers to many written questions [and] conducted extensive interviews with several attorneys who were involved in the review of the President’s program.”
- After carefully considering all of the information available to it, SSCI adopted a bipartisan and measured compromise by a vote of 13 to 2. SSCI did not simply extend the Protect America Act or accept the Administration’s April 2007 proposal.
  - The SSCI legislation was reported out of committee after members had the opportunity to offer amendments, several of which were adopted.
  - This bill enjoys the strong support of the Chairman and Ranking Member of the SSCI.
    - Chairman Rockefeller: “Vice Chairman Bond and I worked very hard over the last few months to produce a bill that both sides could support. While neither side got everything we wanted, at the end of the day, we believe we’ve accomplished what we set out to do – allow for necessary intelligence collection while maintaining critical privacy protections for Americans.”
    - Ranking Member Bond: “I commend Chairman Rockefeller and the members of the Committee for all of their hard work and diplomacy in putting together this important bipartisan compromise. This bill protects American civil liberties while giving our intelligence and law enforcement agencies the tools and agility they need to intercept terrorist communications.”
  - Senators Hatch, Feinstein, and Whitehouse voted for this legislation.
- The SSCI legislation was accompanied by a thoughtful Committee Report, explaining clearly and cogently the reasons for the provisions included in the bill.
- Although there is still work to be done to improve the SSCI legislation, it would continue the ability to target foreign terrorists and other targets believed to be located outside the United States without individualized court orders.

**Cardin (COE07G60) (2-Year Sunset):**

**Summary:**

- Changes sunset of the legislation from 2013 to 2009 (2 year sunset).
- Does not amend provisions concerning the transition following the sunset (i.e. the sections detailing what happens to orders in effect in 2013).

**Discussion:**

- Any sunset introduces a significant level of uncertainty to the rules employed by our intelligence professionals and followed by our private partners.
- There has been extensive public discussion and consideration of FISA modernization and there is now a lengthy factual record on the need for this legislation.
- In particular, a short two year sunset would leave this area of the law in a continuing state of doubt and could cause our private partners to resist cooperating with our intelligence efforts.
- It also could result in the unnecessary expenditure of resources involved in creating new policies and procedures and conducting training each time the law changes.
- The Intelligence Community operates much more effectively when the rules governing our intelligence professionals' ability to track our enemies are established and are not constantly changing.

**Cardin (COE07G61) (IG Audit):**

**Summary:**

- Requires the DOJ IG to complete an audit within 180 days of "all programs of the Federal Government involving the acquisition of communications without a court order on or after September 11, 2001, including the Terrorist Surveillance Program."
- "Such audit shall include acquiring all documents relevant to such programs, including memoranda concerning the legal authority of a program, authorizations of a program, certifications to telecommunications carriers, and court orders."
- The IG shall forward this report to Congress (Judiciary and Intelligence Committees of the House and Senate) within 30 days.
- DNI is to assist in expediting the process of obtaining security clearances.

**Discussion:**

- This provision is unnecessary. The agencies of the Intelligence Community have their own Inspectors General, and the congressional intelligence committees and the Senate Judiciary Committee have been briefed on the Terrorist Surveillance Program described by the President.
- Moreover, certain Congressional Committees have conducted substantial and substantive oversight. For example, the SSCI held seven oversight hearings concerning this program, took testimony from telecommunications carriers, met with Inspectors General, and reviewed sensitive documentation.
- The Senate Judiciary Committee also has received briefings and reviewed the relevant documentation.

**Cardin (COE07G62) (4-Year Sunset):**

**Summary:**

- Changes sunset of the legislation from 2013 to 2011 (4 year sunset).
- Does not amend provisions concerning the transition following the sunset (i.e. the sections detailing what happens to orders in effect in 2013)

**Discussion:**

- Any sunset introduces a significant level of uncertainty to the rules employed by our intelligence professionals and followed by our private partners.
- There has been extensive public discussion and consideration of FISA modernization and there is now a lengthy factual record on the need for this legislation.
- A short sunset would leave this area of the law in a continuing state of doubt and could cause our private partners to resist cooperating with our intelligence efforts.
- It also could result in the unnecessary expenditure of resources involved in creating new policies and procedures and conducting training each time the law changes.
- The Intelligence Community operates much more effectively when the rules governing our intelligence professionals' ability to track our enemies are established and are not constantly changing.

## Feinstein (HEN07K61) (Exclusive Means):

### Summary:

- States that FISA “shall be the exclusive means for targeting the communications or communications information of United States persons for foreign intelligence purposes, whether such persons are inside the United State or outside the United States.”
- Makes Chapters 119 and 121 of title 18 (pertaining to criminal wiretaps and stored communications) and FISA “the exclusive means by which electronic surveillance (as defined in section 101(f), regardless of the limitation of section 701) and the interception of domestic wire, oral, or electronic communications may be conducted.”
- These two limitations are exclusive and apply unless “specific statutory authority for electronic surveillance,” other than an amendment to FISA, is enacted.
- Amends 18 USC § 2511(2)(a)(ii)<sup>1</sup> by adding a separate certification requirement if the assistance sought (information, facilities, or technical assistance) is for foreign intelligence purposes.
  - In addition to stating that a warrant is not required, that all statutory requirements have been met, and that specified assistance is required, the certification from the AG or an official listed in 18 USC § 2518(7) must also “identify the specific provision within [FISA] that provides an exception from providing a court order” and certify that the statutory requirements of that provision have been met.
- Amends the criminal provisions of FISA (50 USC § 1809(a)) by replacing “authorized by statute” with “authorized by this title or chapter 119, 121, or 206 of title 18.”<sup>2</sup>

### Discussion:

- The SSCI bill already has an exclusive means provision.
- This provision in many respect mirrors a highly objectionable provision in the substitute amendment.
- As drafted, it could eliminate the Government’s ability to use some common criminal investigative tools in international terrorism or espionage investigations. These include:

---

<sup>1</sup> The amendment actually references section 2511(2)(a)(i), but that section does not have an (A) or (B), which the amendment references. Section (2)(a)(ii), however, has an (A) and (B) and fits the context of the content of the amendment.

<sup>2</sup> Currently, criminal liability attaches if an individual: (1) engages in electronic surveillance under color of law, unless it is “authorized by statute”; or (2) discloses or uses information when that individual knows or has reason to know the information was obtained through electronic surveillance not “authorized by statute.” 50 USC § 1809.



- Title III Criminal Wiretaps.
  - Criminal Pen Registers and Trap and Trace Devices.
  - Search Warrants.
  - Grand Jury Subpoenas.
- It would eliminate the Government's ability to use certain investigative tools created for national security investigations, like National Security Letters, to collect communications information.
  - It could eliminate the Government's ability to use other investigative tools—including possibly court orders authorizing the access of stored communications—in certain national security investigations.
  - This provision could also disrupt highly classified intelligence activities and could harm the national security. Among other things, ambiguities in critical terms and formulations in the provision—including the term “communications information” (a term that is not defined in FISA) and the introduction of the concept of targeting communications (as opposed to persons)—could lead the statute to bar or require court approval for overseas intelligence activities that involve the incidental collection of U.S. person information.
  - The amendment to the section 2511(2)(a)(ii) certification provision contains ambiguities that could harm the Government's ability to obtain the assistance of our private partners.
  - The amendment to section 1809 would effectively prohibit Congress from passing, in an emergency situation, a law to authorize the immediate collection of communications in the aftermath of an attack or in response to a grave threat to the national security. Instead, it would require Congress to amend one of the specified provisions, which is much more complicated and time-consuming. It is unwise to tie the hands of a future Congress in this manner.

**Kennedy (JEN07G01) (Sunset):**

**Summary:**

- Would change the sunset date of the SSCI legislation from 2013 (6 years from now) to 2009 (two years from now).

**Discussion:**

- Any sunset introduces a significant level of uncertainty to the rules employed by our intelligence professionals and followed by our private partners.
- There has been extensive public discussion and consideration of FISA modernization and there is now a lengthy factual record on the need for this legislation.
- In particular, a short two year sunset would leave this area of the law in a continuing state of doubt and could cause our private partners to resist cooperating with our intelligence efforts.
- It also could result in the unnecessary expenditure of resources involved in creating new policies and procedures and conducting training each time the law changes.
- The Intelligence Community operates much more effectively when the rules governing our intelligence professionals' ability to track our enemies are established and are not constantly changing.

**Kennedy (JEN07G02) (IG Audit):**

**Summary:**

- Would require the DOJ IG to complete an unclassified audit (with a classified annex) within 180 days, of all government programs that involve the acquisition of communications without a court order on or after 9/11/01, including the TSP described by the President. The audit would include acquiring all documents relevant to such programs. The audit and the documents are required to be submitted to HPSCI, SSCI, HJC, and SJC. The DNI is also required to expedite security clearances necessary for such an audit.

**Discussion:**

- This provision is unnecessary. The agencies of the Intelligence Community have their own Inspectors General, and the congressional intelligence committees and the Senate Judiciary Committee have been briefed on the Terrorist Surveillance Program described by the President.
- Moreover, certain Congressional Committees have conducted substantial and substantive oversight. For example, the SSCI held seven oversight hearings concerning this program, took testimony from telecommunications carriers, met with Inspectors General, and reviewed sensitive documentation.
- The Senate Judiciary Committee also has received briefings and reviewed the relevant documentation.

**Kennedy (HEN07K66) (Domestic Communications):**

**Summary:**

- Would prohibit any acquisition under the new authority from resulting in the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of the acquisition to be located in the United States (and makes conforming amendments).
- Would require that the targeting procedures be reasonably designed to ensure that any acquisition under the new authority "not result in the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."
- Would also require that the minimization procedures for the new authority to require the destruction of any communication in which the sender and all intended recipients are known to be located in the United States, where a person has a reasonable expectation of privacy, and a warrant would be required for law enforcement purposes, unless the AG determines that the communication indicates a threat of death or serious bodily injury to any person:

**Discussion:**

- This amendment is aimed at prohibiting the acquisition of domestic to domestic communications under the new acquisition authorities.
- The prohibition is unnecessary because such acquisitions would, pursuant to the SSCI bill, qualify as electronic surveillance under FISA and could not be conducted under the new authorities.
- The provision regarding minimization procedures also is not necessary, because section 1806(i) of FISA already requires the destruction of such communications collected without a court order, and that section applies to information acquired under the new authority. *See* S. 2248, § 704.
- Introduction of new provisions that duplicate existing law will lead to ambiguity and confusion, particularly if courts try to give them a meaning different from those provisions that already exist.

**Kennedy (HEN07K65) (Reverse Targeting):**

**Summary:**

- Would strike the current reverse targeting provision in the SSCI bill (and conforming amendments) to make it read (with key change underlined): [an acquisition under the new authority] “may not intentionally target a person reasonably believed to be outside the United States if a significant purpose of such acquisition is to acquire the communications of a specific person reasonably believed to be located in the United States, except in accordance with title I.”

**Discussion:**

- The concern animating this proposal—that of so-called “reverse targeting,” whereby the government surveils a person overseas when it is really interested in a person in the United States the person overseas is communicating with—is already addressed in current law and the SSCI bill.
- Whenever the person in the United States is the target, an order from the FISA court is required; the SSCI bill codifies this longstanding Executive Branch interpretation of FISA.
- The introduction of an ambiguous and subjective “significant purpose” standard could raise operational uncertainties and problems that make it more difficult to collect intelligence in situations when a foreign terrorist overseas is calling into the United States—which is, of course, precisely the communication we care most about.

**Feingold (HEN07K41) (Exclusivity):**

**Summary:**

- This amendment would amend section 1809 of FISA to clarify that FISA and the criminal wiretap laws are the exclusive means for conducting electronic surveillance.
- Section 1809 currently provides that it is unlawful to engage in electronic surveillance under the color of law "except as authorized by statute."
- It would do this by replacing the phrase "authorized by statute" with "authorized by this title or chapter 119, 121, or 206 of title 18, United States Code."

**Discussion:**

- The SSCI bill already has an exclusive means provision.
- The amendment to section 1809 would effectively prohibit Congress from passing, in an emergency situation, a law to authorize the immediate collection of communications in the aftermath of an attack or in response to a grave threat to the national security. Instead, it would require Congress to amend one of the specified provisions, which is much more complicated and time-consuming. It is unwise to tie the hands of a future Congress in this manner.

**Feingold (HEN07K46) (Limits Type of FI Disseminated):**

**Summary:**

- This amendment would limit the dissemination of US person information acquired under the new authorities to foreign intelligence information as defined in 50 USC § 1801(e)(1).
- Section 1801(e)(1) includes:
  - “(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
    - (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
    - (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
    - (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.”
- This amendment would not allow the dissemination of the foreign intelligence information defined under section 1801(e)(2).
- Section 1801(e)(2) includes:
  - “(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
    - (A) the national defense or the security of the United States; or
    - (B) the conduct of the foreign affairs of the United States.”

**Discussion:**

- This is similar to, but even worse than, unacceptable provisions in the House bill—the RESTORE Act.
- Since 1978, FISA has provided for the collection and dissemination of foreign intelligence information as defined in both parts (1) and (2) of section 1801(e).
- There is no reason to limit the types of intelligence that can be collected from foreigners outside the United States under this authority.
- This is an arbitrary and dangerous limitation—we should not limit the Government’s ability to disseminate information “necessary . . . to the security of the United States.” It is surpassing strange to authorize the intelligence community to collect this information on foreign targets, but then not to allow them to disseminate it.
- This limitation would serve only to require intelligence analysts to spend valuable time and resources distinguishing between types of foreign intelligence information being collected and could place the court in the position of reviewing such operational determinations.

- In addition, terrorist groups and other threats to the national security are not separate phenomena. Thus, the types of foreign intelligence information referenced in section 1801(e) often overlap.



**Feingold (HEN07K49) (Incidentally Acquired USP Communications):**

**Summary:**

- This amendment would require the Government to sequester any communication acquired under the new authority that has been sent to, or received by, a person in the United States.
- The communication would be sequestered "under the authority of" the FISA Court and the Government could only access such communications under an order pursuant to title I of FISA or an emergency exception.
- Under the emergency exception, the Government would have 7 days in which to access the communication and disseminate related foreign intelligence without a court order.
- The AG would be required to submit procedures to the FISA Court to ensure that the court is notified immediately of each instance of emergency access and the court would have to approve those procedures.
- After 7 days, the Government would either have to submit an application for an order "pursuant to title I" or submit documentation explaining why it has not sought an order.
- The amendment would require the Attorney General to adopt additional procedures for determining whether a communication acquired under the new authority has been sent to or received by a person in the United States.
- The amendment also requires destruction of any communication accessed in an emergency if no court order is sought and the Government has not submitted documentation explaining why an order has not been sought, and it permits the FISA Court to prohibit future emergency access to communications with respect to a particular target if the Court determines that the Government has incorrectly invoked the emergency exception.

**Discussion:**

- If enacted, this proposal would destroy the purpose of the Protect America Act, the Intelligence committee bill and the substitute. It is unsound as a matter of policy and is wholly unworkable. In practice, it would limit the authority that could be collected to "foreign-to-foreign" communications. Since the intelligence community often does not know in advance whom a terrorist overseas will communicate with, such a limitation has the effect of gutting the critical tools provided in the Protect America Act.
- Moreover, even if it were operationally feasible (which it is not), it is highly problematic as a matter of policy. It would diminish our ability to swiftly surveil a communication from a terrorist overseas to a person in the U.S.—and that is precisely the communication that the intelligence community needs to move on immediately.

- The concern motivating this proposal—a concern about incidentally collected U.S. person communications—is not a new one 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—and if that were required, there would be grave operational consequences for the intelligence community’s signals intelligence efforts.

**Feingold (HEN07K73) (Bulk Collection):**

**Summary:**

- This amendment aims to prevent “bulk” collection under the new authorities.
- It would require the AG and the DNI to certify for any acquisition that it does not “include communications in which the sender or any intended recipient is reasonably believed to be located inside the United States unless the target is an individual sender or intended recipient of the communication” who is believed to be outside the United States.
- It also would require the certification to state that a “significant purpose” of the acquisition of the target’s communications is to obtain foreign intelligence information.

**Discussion:**

- The amendment is unnecessary; the SSCI bill already provides that the Government cannot, under subsection 703(a), intentionally target any person known at the time of the acquisition to be in the United States.
- The amendment could create ambiguities regarding the scope of authorized activities under the act and could have significant unintended operational consequences.

**Feingold (HEN07K76) (Significant Purpose Limit):**

**Summary:**

- This amendment would require a FISA Court order 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 U.S.
- It also would require the targeting procedures to reflect this requirement.

**Discussion:**

- The concern animating this proposal—that of so-called “reverse targeting,” whereby the government surveils a person overseas when it is really interested in a person in the United States the person overseas is communicating with—is already addressed in current law.
- Whenever the person in the United States is the target, an order from the FISA court is required; the SSCI bill codifies this longstanding Executive Branch interpretation of FISA.
- The introduction of an ambiguous and subjective “significant purpose” standard could raise operational uncertainties and problems that make it more difficult to collect intelligence in situations when a foreign terrorist overseas is calling into the United States—which is, of course, precisely the communication we care most about.

**Feingold (JEN07G06) (Two Year Sunset):**

**Summary:**

- This amendment would sunset the new authority on December 31, 2009.

**Discussion:**

- Any sunset introduces a significant level of uncertainty to the rules employed by our intelligence professionals and followed by our private partners.
- There has been extensive public discussion and consideration of FISA modernization and there is now a lengthy factual record on the need for this legislation.
- In particular, a short two year sunset would leave this area of the law in a continuing state of doubt and could cause our private partners to resist cooperating with our intelligence efforts.
- It also could result in the unnecessary expenditure of resources involved in creating new policies and procedures and conducting training each time the law changes.
- The Intelligence Community operates much more effectively when the rules governing our intelligence professionals' ability to track our enemies are established and are not constantly changing.

**Feingold (JEN07G07) (Classified Information Protections):**

**Summary:**

- The bill currently provides that the FISA Court, upon the request of the Government, “shall” review *ex parte* and *in camera* any Government submission or portion of a submission “which may include classified information.”
- The amendment would replace “shall” with “may,” thereby removing the requirement for the court to review such submissions *ex parte* and *in camera*.

**Discussion:**

- This provision significantly reduces the protections for highly classified information in the SSCI bill. Various similar provisions of FISA itself use the “shall” formulation, and it is unclear why classified information concerning the newly provided information is entitled to any less protection.
- By creating flexibility in the FISC’s review of information the Government believes to be classified and sensitive in nature, the amendment increases the risk of disclosing sensitive information to unintended parties and increases the possibility of conflict over the Government’s determination that the release of the information would cause harm to the national security—a determination that the Executive is best suited to make.

**Feingold (JEN07G08) (Additional Reporting):**

**Summary:**

- This amendment would expand the new reporting requirements in the bill that require the Government to provide a copy of any decision, order, or opinion by the FISA Court or FISA Court of Review that includes a significant construction or interpretation of any provision of FISA.
- The amendment would require the submission of such documents from the last five years before enactment of this bill.

**Discussion:**

- This amendment was offered in SSCI and defeated.
- The reporting requirements in existing law are sufficient to allow Congress to conduct meaningful oversight of intelligence activities under FISA.
- Creating a requirement to submit documentation regarding court orders issued prior to this provision's enactment and without an obvious execution mechanism is unusual and impractical.

**Feingold (JEN07G21) (Minimization Compliance Enforcement):**

**Summary:**

- This amendment would grant the FISA Court explicit authority to issue orders limiting the acquisition, retention, use, or dissemination of information acquired under the new authority if the court finds “non-compliance” with the minimization procedures.

**Discussion:**

- This proposal could place the FISA Court in a position where it would be obligated to 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 (where the court approves surveillance targeting a specific person located in the United States), it is anomalous here, where the court’s role is in approving generally applicable procedures rather than individual surveillances.
- Unlike in the FISA Court’s traditional role of approving and disapproving specific applications, this authority could extend to and affect all surveillance carried out under a particular set of targeting or minimization procedures.



**Specter (GRA07H03) (Signing statements):**

**Summary:**

- “In determining the meaning of this Act, no Federal or State court shall rely on or defer to a presidential signing statement as a source of authority.”

**Discussion:**

- Since at least 1821, Presidents have used signing statements to explain their interpretation of and responsibilities under newly enacted laws, and to guide subordinate officers within the Executive Branch. They are an essential part of the constitutional dialogue between the branches. Most Presidents have issued signing statements; every President since Franklin Roosevelt has done so.
- Because Presidents are sworn to “preserve, protect, and defend the Constitution,” U.S. Const., Art. II, § 1, they have long used signing statements for the purpose of informing Congress and the public when the President believes that a particular provision may be unconstitutional in certain applications, or for saying that he will interpret or execute provisions in a manner that would avoid possible constitutional infirmities.
  - As Assistant Attorney General Walter Dellinger noted during the Clinton Administration, “[s]igning statements have frequently expressed the President’s intention to construe or administer a statute in a particular manner (often to save the statute from unconstitutionality).”
- Signing statements merely explain the President’s interpretation of and responsibilities under the law. The President does not pick and choose the provisions he enforces; he faithfully enforces the law consistent with the Constitution.
- While we have not taken a formal position on this amendment, we have concerns about its constitutionality, because it purports to restrict the independence of our nation’s judiciary by seeking to prohibit the courts from considering signing statements—alone among all interpretive sources—in construing statutes.
- We have not yet fully analyzed the issue, but recommend that Congress proceed with caution before enacting legislation regulating the internal deliberations of the courts, particularly when it singles out for disfavored treatment the statements of only one of the co-equal branches of government.

## **Specter (GRA07G93) (Signing statements):**

### **Summary:**

- “In determining the meaning of this Act, no Federal or State court shall rely on or defer to a presidential signing statement as a source of authority.”
- If the President issues a signing statement regarding the Act, Congress may submit an amicus curiae brief in any action construing or affecting the constitutionality of the Act. Congress may also pass a concurrent resolution offering its interpretation and may offer that resolution as part of the record of any judicial proceeding that is construing or considering the constitutionality of the Act.

### **Discussion:**

- Since at least 1821, Presidents have used signing statements to explain their interpretation of and responsibilities under newly enacted laws, and to guide subordinate officers within the Executive Branch. They are an essential part of the constitutional dialogue between the branches. Most Presidents have issued signing statements; every President since Franklin Roosevelt has done so.
- Because Presidents are sworn to “preserve, protect, and defend the Constitution,” U.S. Const., Art. II, § 1, they have long used signing statements for the purpose of informing Congress and the public when the President believes that a particular provision may be unconstitutional in certain applications, or for saying that he will interpret or execute provisions in a manner that would avoid possible constitutional infirmities.
  - As Assistant Attorney General Walter Dellinger noted during the Clinton Administration, “[s]igning statements have frequently expressed the President’s intention to construe or administer a statute in a particular manner (often to save the statute from unconstitutionality).”
- Signing statements merely explain the President’s interpretation of and responsibilities under the law. The President does not pick and choose the provisions he enforces; he faithfully enforces the law consistent with the Constitution.
- While we have not taken a formal position on this amendment, we have concerns about its constitutionality; because it purports to restrict the independence of our nation’s judiciary by seeking to prohibit the courts from considering signing statements—alone among all interpretive sources—in construing statutes.
- We have not yet fully analyzed the issue, but recommend that Congress proceed with caution before enacting legislation regulating the internal deliberations of the courts, particularly when it singles out for disfavored treatment the statements of only one of the co-equal branches of government.

## Specter (GRA07G95) (Signing statements):

### Summary:

- “In determining the meaning of this Act, no Federal or State court shall rely on or defer to a presidential signing statement as a source of authority.”
- If President issues a signing statement regarding the Act, Congress may submit an amicus curiae brief in any action construing or affecting the constitutionality of the Act. Congress may also pass a concurrent resolution offering its interpretation and may offer that resolution as part of the record of any judicial proceeding that is construing or considering the constitutionality of the Act.
- If the President has issued a signing statement concerning the Act and if a matter before the Supreme Court would require it to construe or consider the constitutionality of the Act, the Supreme Court is to notify Congress, and Congress is to have the right to intervene and offer evidence.

### Discussion:

- Since at least 1821, Presidents have used signing statements to explain their interpretation of and responsibilities under newly enacted laws, and to guide subordinate officers within the Executive Branch. They are an essential part of the constitutional dialogue between the branches. Most Presidents have issued signing statements; every President since Franklin Roosevelt has done so.
- Because Presidents are sworn to “preserve, protect, and defend the Constitution,” U.S. Const., Art. II, § 1, they have long used signing statements for the purpose of informing Congress and the public when the President believes that a particular provision may be unconstitutional in certain applications, or for saying that he will interpret or execute provisions in a manner that would avoid possible constitutional infirmities.
  - As Assistant Attorney General Walter Dellinger noted during the Clinton Administration, “[s]igning statements have frequently expressed the President’s intention to construe or administer a statute in a particular manner (often to save the statute from unconstitutionality).”
- Signing statements merely explain the President’s interpretation of and responsibilities under the law. The President does not pick and choose the provisions he enforces; he faithfully enforces the law consistent with the Constitution.
- While we have not taken a formal position on this amendment, we have concerns about its constitutionality, because it purports to restrict the independence of our nation’s judiciary by seeking to prohibit the courts from considering signing statements—alone among all interpretive sources—in construing statutes.
- We have not yet fully analyzed the issue, but recommend that Congress proceed with caution before enacting legislation regulating the internal deliberations of the courts, particularly when it singles out for disfavored treatment the statements of only one of the co-equal branches of government.

## Specter (GRA07G97) (Signing statements):

### Summary:

- “In determining the meaning of this Act, no Federal or State court shall rely on or defer to a presidential signing statement as a source of authority.”
- If President issues a signing statement regarding the Act, Congress may submit an amicus curiae brief in any action construing or affecting the constitutionality of the Act. Congress may also pass a concurrent resolution offering its interpretation and may offer that resolution as part of the record of any judicial proceeding that is construing or considering the constitutionality of the Act.
- If the President has issued a signing statement with respect to FISA, the Senate or the House may seek a declaratory judgment regarding the legality of that statement.

### Discussion:

- Since at least 1821, Presidents have used signing statements to explain their interpretation of and responsibilities under newly enacted laws, and to guide subordinate officers within the Executive Branch. They are an essential part of the constitutional dialogue between the branches. Most Presidents have issued signing statements; every President since Franklin Roosevelt has done so.
- Because Presidents are sworn to “preserve, protect, and defend the Constitution,” U.S. Const., Art. II, § 1, they have long used signing statements for the purpose of informing Congress and the public when the President believes that a particular provision may be unconstitutional in certain applications, or for saying that he will interpret or execute provisions in a manner that would avoid possible constitutional infirmities.
  - As Assistant Attorney General Walter Dellinger noted during the Clinton Administration, “[s]igning statements have frequently expressed the President’s intention to construe or administer a statute in a particular manner (often to save the statute from unconstitutionality).”
- Signing statements merely explain the President’s interpretation of and responsibilities under the law. The President does not pick and choose the provisions he enforces; he faithfully enforces the law consistent with the Constitution.
- While we have not taken a formal position on this amendment, we have concerns about its constitutionality, because it purports to restrict the independence of our nation’s judiciary by seeking to prohibit the courts from considering signing statements—alone among all interpretive sources—in construing statutes.
- We have not yet fully analyzed the issue, but recommend that Congress proceed with caution before enacting legislation regulating the internal deliberations of the courts, particularly when it singles out for disfavored treatment the statements of only one of the co-equal branches of government.

**Specter (HEN07K29) (Substitution):**

**Summary:**

- If the Attorney General issues a certification pursuant to section 201(3)(B), the United States will be substituted as the party defendant for any covered civil action against a telecommunications provider.
- Allows a telecommunications provider to petition a court to determine that the United States should be substituted in the event the Attorney General has not issued a 201(3)(B) certification.
- Provides for the removal of actions from state to Federal court if the Attorney General issues a certification or if a telecommunications provider petitions the court for substitution.

**Discussion:**

- Companies that are alleged to have done nothing more than assisted the government in good faith would still face many of the burdens of litigation, such as discovery and document production. The companies could also suffer damage to their business reputations as a result of their continued involvement in the lawsuits.
- Allowing these suits to continue risks the further disclosure of highly classified information.
- The lawsuits could result in an expenditure of taxpayer resources, as the result of any adverse judgment would likely be the shifting of money from the Treasury to a large group of class action plaintiffs.
- Because the United States would be substituted only where the carrier defendant provided assistance pursuant to a written request, and because a carrier defendant could petition the court for a finding that there should be substitution, this Amendment would make it difficult, if not possible, for the United States to assert the state secrets privilege over (a) whether it was engaged in an alleged intelligence activity and/or (b) whether a particular carrier provided assistance for that alleged activity.
- Provision is completely silent on how suits against the United States would proceed after substitution.

**Specter (HEN07K42) (FISC Review of Targeting and Minimization Compliance):**

**Summary:**

- Requires the FISA Court to review targeting and minimization procedures to determine whether they meet the relevant definition (101(h)) or standard contained in this legislation (reasonably designed to determine if a target is reasonably located outside of the United States).
- Requires the FISC, after receiving a semiannual report from the AG and DNI or an annual review from an agency, to determine whether targeting and minimization procedures are "being fulfilled." FISC has the authority to "require action" to correct any deficiencies it may identify.

**Discussion:**

- This proposal could place the FISA Court in a position where it would be authorized to 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 (where the court approves surveillance targeting a specific person located in the United States), it is anomalous here, where the court's role is in approving generally applicable procedures rather than individual surveillances.
- Providing the Court with the broad (and seemingly unreviewable) authority to "require action" to correct any deficiencies it may identify would introduce substantial uncertainty into the collection of foreign intelligence.
- Unlike the FISA Court's traditional role of approving and disapproving specific applications, this authority would extend to and affect all surveillance carried out under a particular set of targeting or minimization procedures.

**Specter (HEN07K56) (FISC Review of Targeting and Minimization Procedures and Specific Factors FISC Shall Consider):**

**Summary:**

- Requires the FISA Court to review targeting and minimization procedures to determine whether they meet the relevant definition (101(h)) or standard contained in this legislation (reasonably designed to determine if a target is reasonably located outside of the United States).
- As part of these reviews, the FISC shall take into account specific factors, including support materials, prior applications to the Court, prior authorization orders of the Court, semiannual assessments from the AG and DNI, and annual agency reviews.

**Discussion**

- Neither FISA nor the PAA has required the FISC to consider specific factors in evaluating minimization or targeting procedures.
- The PAA and the current SSCI legislation provide standards for the court to follow in approving applications and in reviewing procedures. It is not clear why these particular factors will be relevant to every determination.

**Specter (JEN07F99) (Exclusive Means):**

**Summary:**

- This would modify the exclusivity provision in the SSCI bill by adding:  
“No provision of law shall be construed to implicitly repeal or modify this title or any provision thereof, nor shall any provision of law be deemed to repeal or modify this title in any manner unless such provision of law, if enacted after the date of the enactment of the FISA Amendments Act of 2007, expressly amends or otherwise specifically cites this title.”

**Discussion:**

- Among other things, this provision would impede the ability of Congress, in an emergency situation, to pass a law authorizing the immediate collection of communications in the aftermath of an attack or in response to a grave threat to the national security.
- Instead, it would require Congress to expressly amend or otherwise cite FISA.
- It is unwise to tie the hands of a future Congress in this manner.