



EISENBERG AND HANCOCK, LLP

August 6, 2007

Ms. Cathy Catterson
Clerk, United States Court of Appeals, Ninth Circuit
95 Seventh St.
San Francisco, CA 94103

Re: *Al-Haramain Islamic Foundation, Inc. v. Bush*, No. 06-36083
(Scheduled for oral argument on August 15, 2007)

Dear Ms. Catterson:

Pursuant to Federal Rule of Appellate Procedure 28(j), we call this Court's attention to Senate Bill 1927 (enacted August 5, 2007) and explanatory congressional testimony.

S. 1927 amends FISA in pertinent part to state: "Nothing in the definition of electronic surveillance under [50 U.S.C. § 1801(f)] shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States." See Attachment 1. This provision concerns the definition of "electronic surveillance" in § 1801(f)(2) as "the acquisition . . . of the contents of any wire communication to or from a person in the United States . . . if such acquisition occurs in the United States"

The effect of the amendment is to permit something FISA formerly prohibited – warrantless surveillance of wire communications *where the acquisition occurs in the United States*, even though the person targeted is located outside the United States.

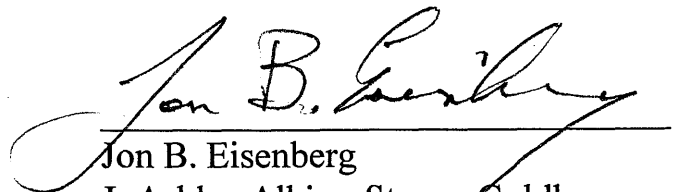
In testimony before the Senate Select Committee on Intelligence, Director of National Intelligence Mike McConnell and NSA Director Keith Alexander explained the reason for the amendment: Because of technological innovations since FISA's inception, communications between persons located inside and outside the United States are now transmitted over wire, and the interception of such communications occurs inside the United States. Thus, according to McConnell, "when seeking to monitor foreign persons suspected of involvement in terrorist activity who are physically located in foreign countries, the intelligence community is required under

today's FISA [50 U.S.C. § 1801(f)(2)] to obtain a court order to conduct surveillance." See Attachment 2.

The communications at issue in *Al-Haramain* were between persons located inside and outside the United States. McConnell's testimony is an admission that those communications were "electronic surveillance" within the meaning of § 1801(f)(2), so that their surveillance required a warrant – a requirement S. 1927 eliminates if the person targeted for surveillance is located outside the United States.

The applicability of § 1801(f)(2) in this case was previously obscured by President Bush's assertion on December 19, 2005, that "these calls are not intercepted within the country." See Attachment 3. McConnell's testimony and the enactment of S. 1927 demonstrate otherwise.

Respectfully submitted,



Jon B. Eisenberg
J. Ashlee Albies, Steven Goldberg,
Lisa R. Jaskol, William Hancock,
Zaha S. Hassan, & Thomas A. Nelson

Attorneys for Plaintiffs and Appellees
**Al-Haramain Islamic Foundation, Inc.,
Wendell Belew, and Asim Ghafoor**

cc: Douglas N. Letter
Thomas Bondy
Anthony Yang
Charles F. Hinkle
Emilie K. Edling

ATTACHMENT 1

The Library of Congress > THOMAS Home > Bills, Resolutions > Search Results

<i>THIS SEARCH</i>	<i>THIS DOCUMENT</i>	<i>GO TO</i>
Next Hit	Forward	New Bills Search
Prev Hit	Back	HomePage
Hit List	Best Sections	Help
	Contents Display	

Bill 2 of 2

There is 1 other version of this bill.

GPO's PDF Display	Congressional Record References	Bill Summary & Status	Printer Friendly Display - 17,465 bytes.[Help]
-----------------------------------	---	---	--

Protect America Act of 2007 (Engrossed as Agreed to or Passed by Senate)

S 1927 ES

110th CONGRESS

1st Session

S. 1927

AN ACT

To amend the Foreign Intelligence Surveillance Act of 1978 to provide additional procedures for authorizing certain acquisitions of foreign intelligence information and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the `Protect America Act of 2007'.

SEC. 2. ADDITIONAL PROCEDURE FOR AUTHORIZING CERTAIN ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION.

The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by inserting after section 105 the following:

` CLARIFICATION OF ELECTRONIC SURVEILLANCE OF PERSONS OUTSIDE THE

UNITED STATES

Sec. 105A. Nothing in the definition of electronic surveillance under section 101(f) shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States.

ADDITIONAL PROCEDURE FOR AUTHORIZING CERTAIN ACQUISITIONS CONCERNING PERSONS LOCATED OUTSIDE THE UNITED STATES

Sec. 105B. (a) Notwithstanding any other law, the Director of National Intelligence and the Attorney General, may for periods of up to one year authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States if the Director of National Intelligence and the Attorney General determine, based on the information provided to them, that--

- (1) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States, and such procedures will be subject to review of the Court pursuant to section 105C of this Act;
- (2) the acquisition does not constitute electronic surveillance;
- (3) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;
- (4) a significant purpose of the acquisition is to obtain foreign intelligence information; and
- (5) the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).

This determination shall be in the form of a written certification, under oath, supported as appropriate by affidavit of appropriate officials in the national security field occupying positions appointed by the President, by and with the consent of the Senate, or the Head of any Agency of the Intelligence Community, unless immediate action by the Government is required and time does not permit the preparation of a certification. In such a case, the determination of the Director of National Intelligence and the Attorney General shall be reduced to a certification as soon as possible but in no event more than 72 hours after the determination is made.

` (b) A certification under subsection (a) is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed.

` (c) The Attorney General shall transmit as soon as practicable under seal to the court established under section 103(a) a copy of a certification made under subsection (a). Such certification shall be maintained under security measures established by the Chief Justice of the United States and the Attorney General, in consultation with the Director of National Intelligence, and shall remain sealed unless the certification is necessary to determine the legality of the acquisition under section 105B.

` (d) An acquisition under this section may be conducted only in accordance with the certification of the Director of National Intelligence and the Attorney General, or their oral instructions if time does not permit the preparation of a certification, and the minimization procedures adopted by the Attorney General. The Director of National Intelligence and the Attorney General shall assess compliance with such procedures and shall report such assessments to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate under section 108(a).

` (e) With respect to an authorization of an acquisition under section 105B, the Director of National Intelligence and Attorney General may direct a person to--

` (1) immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition in such a manner as will protect the secrecy of the acquisition and produce a minimum of interference with the services that such person is providing to the target; and

` (2) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such person wishes to maintain.

` (f) The Government shall compensate, at the prevailing rate, a person for providing information, facilities, or assistance pursuant to subsection (e).

` (g) In the case of a failure to comply with a directive issued pursuant to subsection (e), the Attorney General may invoke the aid of the court established under section 103(a) to compel compliance with the directive. The court shall issue an order requiring the person to comply with the directive if it finds that the directive was issued in accordance with subsection (e) and is otherwise lawful. Failure to obey an order of the court may be punished by the court as contempt of court. Any process under this section may be served in any judicial district in which the person may be found.

` (h)(1)(A) A person receiving a directive issued pursuant to subsection (e) may challenge the legality of that directive by filing a petition with the pool established under section 103(e)(1).

` (B) The presiding judge designated pursuant to section 103(b) shall assign a petition filed under subparagraph (A) to one of the judges serving in the pool

established by section 103(e)(1). Not later than 48 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the directive. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the directive or any part of the directive that is the subject of the petition. If the assigned judge determines the petition is not frivolous, the assigned judge shall, within 72 hours, consider the petition in accordance with the procedures established under section 103(e)(2) and provide a written statement for the record of the reasons for any determination under this subsection.

` (2) A judge considering a petition to modify or set aside a directive may grant such petition only if the judge finds that such directive does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the directive, the judge shall immediately affirm such directive, and order the recipient to comply with such directive.

` (3) Any directive not explicitly modified or set aside under this subsection shall remain in full effect.

` (i) The Government or a person receiving a directive reviewed pursuant to subsection (h) may file a petition with the Court of Review established under section 103(b) for review of the decision issued pursuant to subsection (h) not later than 7 days after the issuance of such decision. Such court of review shall have jurisdiction to consider such petitions and shall provide for the record a written statement of the reasons for its decision. On petition for a writ of certiorari by the Government or any person receiving such directive, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

` (j) Judicial proceedings under this section shall be concluded as expeditiously as possible. The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

` (k) All petitions under this section shall be filed under seal. In any proceedings under this section, the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.

` (l) Notwithstanding any other law, no cause of action shall lie in any court against any person for providing any information, facilities, or assistance in accordance with a directive under this section.

` (m) A directive made or an order granted under this section shall be retained for a period of not less than 10 years from the date on which such directive or such order is made.'.

SEC. 3. SUBMISSION TO COURT REVIEW AND ASSESSMENT OF PROCEDURES.

The Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by inserting after section 105B the following:

` SUBMISSION TO COURT REVIEW OF PROCEDURES

` Sec. 105C. (a) No later than 120 days after the effective date of this Act, the Attorney General shall submit to the Court established under section 103(a), the procedures by which the Government determines that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance. The procedures submitted pursuant to this section shall be updated and submitted to the Court on an annual basis.

` (b) No later than 180 days after the effective date of this Act, the court established under section 103(a) shall assess the Government's determination under section 105B(a)(1) that those procedures are reasonably designed to ensure that acquisitions conducted pursuant to section 105B do not constitute electronic surveillance. The court's review shall be limited to whether the Government's determination is clearly erroneous.

` (c) If the court concludes that the determination is not clearly erroneous, it shall enter an order approving the continued use of such procedures. If the court concludes that the determination is clearly erroneous, it shall issue an order directing the Government to submit new procedures within 30 days or cease any acquisitions under section 105B that are implicated by the court's order.

` (d) The Government may appeal any order issued under subsection (c) to the court established under section 103(b). If such court determines that the order was properly entered, the court shall immediately provide for the record a written statement of each reason for its decision, and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision. Any acquisitions affected by the order issued under subsection (c) of this section may continue during the pendency of any appeal, the period during which a petition for writ of certiorari may be pending, and any review by the Supreme Court of the United States.'

SEC. 4. REPORTING TO CONGRESS.

On a semi-annual basis the Attorney General shall inform the Select Committee on Intelligence of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, the Committee on the Judiciary of the Senate, and the Committee on the Judiciary of the House of Representatives, concerning acquisitions under this section during the previous 6-month period. Each report made under this section shall include--

(1) a description of any incidents of non-compliance with a directive issued by the Attorney General and the Director of National Intelligence under section 105B, to include--

(A) incidents of non-compliance by an element of the Intelligence Community with guidelines or procedures established for determining that the acquisition of foreign intelligence authorized by the Attorney General and Director of National Intelligence concerns persons reasonably to be outside the United States; and

(B) incidents of noncompliance by a specified person to whom the Attorney General and Director of National Intelligence issue a directive under this section; and

(2) the number of certifications and directives issued during the reporting period.

SEC. 5. TECHNICAL AMENDMENT AND CONFORMING AMENDMENTS.

(a) In General- Section 103(e) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(e)) is amended--

(1) in paragraph (1), by striking ` 501(f)(1)' and inserting ` 105B(h) or 501(f)(1)'; and

(2) in paragraph (2), by striking ` 501(f)(1)' and inserting ` 105B(h) or 501(f)(1)'.

(b) Table of Contents- The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by inserting after the item relating to section 105 the following:

` 105A. Clarification of electronic surveillance of persons outside the United States.

` 105B. Additional procedure for authorizing certain acquisitions concerning persons located outside the United States.

` 105C. Submission to court review of procedures.'.

SEC. 6. EFFECTIVE DATE; TRANSITION PROCEDURES.

(a) Effective Date- Except as otherwise provided, the amendments made by this Act shall take effect immediately after the date of the enactment of this Act.

(b) Transition Procedures- Notwithstanding any other provision of this Act, any order in effect on the date of enactment of this Act issued pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall remain in effect until the date of expiration of such order, and, at the request of the applicant, the court established under section 103(a) of such Act (50 U.S.C. 1803(a)) shall reauthorize such order as long as the facts and circumstances continue to justify issuance of such order under the provisions of the Foreign Intelligence Surveillance Act of 1978, as in effect on the day before the applicable effective date of this Act.

The Government also may file new applications, and the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803 (a)) shall enter orders granting such applications pursuant to such Act, as long as the application meets the requirements set forth under the provisions of such Act as in effect on the day before the effective date of this Act. At the request of the applicant, the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)), shall extinguish any extant authorization to conduct electronic surveillance or physical search entered pursuant to such Act. Any surveillance conducted pursuant to an order entered under this subsection shall be subject to the provisions of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), as in effect on the day before the effective date of this Act.

(c) Sunset- Except as provided in subsection (d), sections 2, 3, 4, and 5 of this Act, and the amendments made by this Act, shall cease to have effect 180 days after the date of the enactment of this Act.

(d) Authorizations in Effect- Authorizations for the acquisition of foreign intelligence information pursuant to the amendments made by this Act, and directives issued pursuant to such authorizations, shall remain in effect until their expiration. Such acquisitions shall be governed by the applicable provisions of such amendments and shall not be deemed to constitute electronic surveillance as that term is defined in section 101(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(f)).

Passed the Senate August 3, 2007.

Attest:

Secretary.

110th CONGRESS

1st Session

S. 1927

AN ACT

To amend the Foreign Intelligence Surveillance Act of 1978 to provide additional procedures for authorizing certain acquisitions of foreign intelligence information and for other purposes.

THIS SEARCH

[Next Hit](#)

[Prev Hit](#)

[Hit List](#)

THIS DOCUMENT

[Forward](#)

[Back](#)

[Best Sections](#)

[Contents Display](#)

GO TO

[New Bills Search](#)

[HomePage](#)

[Help](#)

ATTACHMENT 2

**HEARING OF THE SENATE SELECT COMMITTEE ON INTELLIGENCE
PROPOSED FISA MODERNIZATION LEGISLATION**

WITNESSES:

MR. MIKE McCONNELL, DIRECTOR OF NATIONAL INTELLIGENCE;

LTG KEITH ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY;

MR. KENNETH WAINSTEIN, ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY,
DEPARTMENT OF JUSTICE;

MR. BENJAMIN POWELL, GENERAL COUNSEL, OFFICE OF THE DIRECTOR OF NATIONAL
INTELLIGENCE;

MR. VITO POTENZA, GENERAL COUNSEL, NATIONAL SECURITY AGENCY

CHAired BY: SENATOR JOHN D. ROCKEFELLER IV (D-WV)

LOCATION: 106 DIRKSEN SENATE OFFICE BUILDING, WASHINGTON, D.C.

TIME: 2:30 P.M. EDT

DATE: TUESDAY, MAY 1, 2007

SEN. ROCKEFELLER: This hearing has begun, and I welcome all of our testifiers. And other members of the committee will be coming in. I know some of the caucuses just broke up.

The Select Committee on Intelligence meets today in open session, something we don't ought to do, to consider whether the scope and application regarding the Surveillance Act needs to be changed to reflect the evolving needs for the timely collection of foreign intelligence. An extraordinarily complicated subject, this is. At the committee's request, the administration has undertaken a comprehensive review of the Foreign Intelligence Surveillance Act, commonly referred to as FISA. Out of this review, the administration proposed -- it believes would modernize the laws governing the way in which we gather foreign intelligence with the use of electronic surveillance.

Consideration of the administration's proposal and alternatives will be rooted in the Intelligence Committee's 30-year experience with our nation's long and delicate effort to strike that elusive right balance between effective intelligence collection for our national security and the constitutional rights and privacy interests of Americans.

The Intelligence Committee's existence came out of the work of the Church Committee and others in the mid-'70s to bring to light abuses in the electronic surveillance of Americans. One of the committee's first tasks was to work with the Senate Judiciary Committee and with the Ford and Carter administrations from 1976 to 1978 to enact the Foreign Intelligence Surveillance Act. As we take a fresh look at the current law, we will again be working with our colleagues in the Senate Judiciary Committee.

FISA involves both the judicial process on the one hand and the collection of intelligence. Our committee's contribution to this process

MR. MIKE McCONNELL: Good afternoon, Chairman Rockefeller, Vice Chairman Bond, members of the committee. Thank you for inviting us to come today to engage with the Congress on legislation that will modernize the Foreign Intelligence Surveillance Act, as you mentioned, FISA -- I'll refer to it as FISA from this point on -- which was passed in 1978.

In response to your guidance from last year on the need to revise FISA, the administration has worked for over the past year, with many of you and your staff experts, to craft the proposed legislative draft. It will help our intelligence professionals, if passed, protect the nation by preventing terrorist acts inside the United States. Since 1978, FISA has served as the foundation to conduct electronic surveillance of foreign powers or agents of foreign powers inside the United States. We are here today to share with you the criticality -- critical important role that FISA plays in protecting the nation's security, and how I believe the proposed legislation will improve that role, while continuing to protect the civil and the privacy rights of all Americans.

The proposed legislation to amend FISA has four key characteristics. First, it makes the statute technology-neutral. It seeks to bring FISA up to date with the changes in communications technology that have taken place since 1978. Second, it seeks to restore FISA to its original focus on protecting the privacy interests of persons inside the United States. Third, it enhances the government's authority to secure assistance by private entities, which is vital for the intelligence community to be successful. And fourth, it makes changes that will streamline FISA administrative processes so that the intelligence community can use FISA as a tool to gather foreign intelligence information more quickly and more effectively.

The four critical questions, four critical questions that we must address in collection against foreign powers or agents of foreign powers are the following. First, who is the target of the communications? Second, where is the target located? Third, how do we intercept the communications? And fourth, where do we intercept the communications? Where we intercept the communications has become a very important part of the determination that must be considered in updating FISA.

As the committee is aware, I've spent the majority of my professional life in or serving the intelligence community. In that capacity, I've been both a collector of information and a consumer of intelligence information. I had the honor of serving as the director of the National Security Agency from 1992 to 1996. In that position, I was fully aware of how FISA serves a critical function enabling the collection of foreign intelligence information.

In my first 10 weeks on the job as the new director of National Intelligence, I immediately can see the results of FISA-authorized collection activity. The threats faced by our nation, as I have previously testified to this committee, are very complex and there are very many. I cannot overstate how instrumental FISA has been in helping the intelligence community protect the nation from terrorist attacks since September 11th, 2001.

Some of the specifics that support my testimony, as has been mentioned, cannot be discussed in open session. This is because certain information about our capabilities could cause us to lose the capability if known to the terrorists. I look forward to elaborating further on aspects of the issues in a closed session that is scheduled to follow.

I can, however, make the following summary-level comment about the current FISA legislation. Since the law was drafted in a period preceding today's global information technology transformation and does not address today's global systems in today's terms, the intelligence community is significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States.

Let me repeat that for emphasis. We are significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States. We must make the requested changes to protect our citizens and the nation. In today's threat environment, the FISA legislation is not agile enough to handle the community's and the country's intelligence needs. Enacted nearly 30 years ago, it has not kept pace with 21st century developments in communications technology. As a result, FISA frequently requires judicial authorization to collect the communications of non-U.S. -- that is, foreign -- persons located outside the United States.

Let me repeat again for emphasis. As a result, today's FISA requires judicial authorization to collect communications of non-U.S. persons -- i.e., foreigners -- located outside the United States. This clogs the FISA process with matters that have little to do with protecting civil liberties or privacy of persons in the United States. Modernizing FISA would greatly improve that process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

FISA was enacted before cell phones, before e-mail and before the internet was a tool used by hundreds of millions of people worldwide every day.

There are two kinds of communications. It's important to just recapture the fact, two kinds of communications: wire and wireless. It's either on a wire -- could be a copper wire, a fiber wire -- it's on a wire or it's wireless, meaning it's transmitted through the atmosphere.

When the law was passed in 1978, almost all local calls were on a wire. Almost all local calls, meaning in the United States, were on a wire, and almost all long-haul communications were in the air, were known as wireless communications. Therefore, FISA in 1978 was written to distinguish between collection on a wire and collection out of the air or against wireless.

Now in the age of modern communications today, the situation is completely reversed. It's completely reversed. Most long-haul communications -- think overseas -- are on a wire -- think fiberoptic pipe. And local calls are in the air. Think of using your cell phone for mobile communications.

Communications technology has evolved in ways that have had unforeseen consequences under FISA, passed in 1978. Technological changes have brought within FISA's scope communications that we believe the 1978 Congress did not intend to be covered. In short, communications currently fall under FISA that were originally excluded from the act. And that is foreign-to-foreign communications by parties located overseas.

The solution is to make FISA technology-neutral. Just as the Congress in 1978 could not anticipate today's technology, we cannot know what technology may bring in the next thirty years. Our job is to make the country as safe as possible by providing the highest quality intelligence available. There is no reason to tie the nation's security to a snapshot of outdated technology.

Additionally, FISA places a premium on the location of the collection. Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today, a single communication can transit the world even if the two people communicating are only located a few miles apart. And yet simply because our law has not kept pace with technology, communications intended to be excluded from FISA are in fact included. There is no real consequence -- this has real consequence on the intelligence community working to protect the nation.

Today intelligence agencies may apply, with the approval of the attorney general and the certification of other high level officials, for court orders to collect foreign intelligence information under FISA. Under the existing FISA statute, the intelligence community is often required to make a showing of probable cause.

Frequently, although not always, that person's communications are with another foreign person overseas. In such cases, the statutory requirement is to obtain a court order, based on a showing of probable cause, that slows, and in some cases prevents altogether, the government's effort to conduct surveillance of communications it believes are significant to national security, such as a terrorist coordinating attacks against the nation located overseas.

This is a point worth emphasizing, because I think many Americans would be surprised at what the current law requires. To state the case plainly: when seeking to monitor foreign persons suspected of involvement in terrorist activity who are physically located in foreign countries, the intelligence community is required under today's FISA to obtain a court order to conduct surveillance. We find ourselves in a position, because of the language in the 1978 FISA statute, simply -- we have not kept pace with the revolution in communications technology that allows the flexibility we need.

As stated earlier, this committee and the American people should know that the information we are seeking is foreign intelligence information. Specifically, this includes information relating to the capabilities, intentions and activities of foreign powers or agents of foreign powers, including information on international terrorist activities. FISA was intended to permit the surveillance of foreign intelligence targets while providing appropriate protection through court supervision to U.S. citizens and other persons located inside the United States.

Debates concerning the extent of the president's constitutional powers were heated in the mid-'70s, as indeed they are today. We believe that the judgment of the Congress at that time was that the FISA regime of court supervision was focused on situations where Fourth Amendment interests of persons in the United States were implicated. Nothing -- and I would repeat -- nothing in the proposed legislation changes this basic premise in the law.

complete understanding of how the statute has been interpreted and how it's being currently used. I don't know how you legislate that way. MR. WAINSTEIN: Well, I understand, but obviously, every time they issue an order, that is -- that can be an interpretation of how the FISA statute is -- interpretation of the FISA statute. And as you know from the numbers that we issue, we have a couple thousand FISAs a year. So that would be quite a few documents.

SEN. FEINGOLD: This is an important matter. If that's the number of items we need to look at, that's the number we will look at.

Thank you, Mr. Chairman.

SEN. ROCKEFELLER: Thank you, Senator Feingold.

Senator Nelson.

SEN. BILL NELSON (D-FL): Mr. Chairman, most of my questions I'm going to save for the closed session, but I would like to ascertain the administration's state of mind with regard to the current law. In the case where there is a foreign national in a foreign land calling into the United States, if you do not know the recipient's nationality and therefore it is possible it is a U.S. citizen, do you have to, in your interpretation of the current law, go and get a FISA order?

MR. McCONNELL: No, sir, not if it -- if the target is in a foreign country and our objective is to collect against the foreign target, and they call into the United States, currently it would not require a FISA. And let me double-check that. I may be -- I'm dated.

LTG ALEXANDER: If it's collected in the United States, it would require a FISA if we do not know who the end is to, or under the program it would have to be collected. If it were known, both ends foreign, known a priori, which is hard to do in this case, you would not. If it was collected overseas, you would not.

SEN. BILL NELSON: Let's go back to your second -- General, your second answer.

LTG ALEXANDER: If you know both ends -- where the call is going to go to before he makes the call, then you know that both ends were foreign; if you knew that ahead of time, you would not need a warrant.

SEN. NELSON: If you knew that.

LTG ALEXANDER: If you knew that.

SEN. NELSON: If you did not know that the recipient of the call in the U.S. is foreign, then you would have to have a FISA order.

LTG ALEXANDER: If you collected it in the United States. If you collected it overseas, you would not.

SEN. NELSON: Well, since in digital communications, if these things -- little packets of information are going all over the globe, you might be collecting it outside the United States, you might be collecting it inside the United States.

MR. McCONNELL: And Senator, that's our dilemma. In the time in 1978 when it was passed, almost everything in the United States was wire, and it was called electronic surveillance. Everything external in the United States was in the air, and it was called communications intelligence.

So what changed is now things in the United States are in the air, and things outside are on wire. That's the --

SEN. NELSON: I understand that, but -- now, I got two different answers to the same question from you, Mr. Director, and from you, General.

MR. McCONNELL: It depends on where the target is and where you collect it. That's why you heard different answers.

SEN. NELSON: So if you're collecting the information in the United States --

MR. McCONNELL: It requires a FISA.

SEN. NELSON: Okay. Under the current law, the president is allowed 72 hours in which he can go ahead and collect information and, after the fact, go back and get the FISA order.

Why was that suspended before in the collection of information?

LTG ALEXANDER: Sir, I think that would best be answered in closed session to give you exactly the correct answer, and I think I can do that.

SEN. NELSON: And -- well, then, you can acknowledge here that is -- it was in fact suspended.

SEN. ROCKEFELLER: I would hope that that would be -- we would leave this where it is.

SEN. NELSON: All right. I'll just stop there.

SEN. ROCKEFELLER: Thank you, Senator Nelson.

Senator Feinstein.

SEN. DIANNE FEINSTEIN (D-CA): Thank you very much, Mr. Chairman. The administration's proposal, Admiral, doesn't address the authority that the president and attorney general have claimed in conducting electronic surveillance outside of FISA. While the FISA Court issued a ruling that authorized the surveillance ongoing under the so-called TSP, Terrorist Surveillance Program, the White House has never acknowledged that it needs court approval. In fact, the president, under this reasoning, could restart the TSP tomorrow without court supervision if he so desired.

Now, Senator Specter and I have introduced legislation which very clearly establishes that FISA is the exclusive authority for conducting intelligence in the United States.

Here's the question: Does the administration still believe that it has the inherent authority to conduct electronic surveillance of the type done under the TSP without a warrant?

ATTACHMENT 3

The President's News Conference

December 19, 2005

The President. Welcome. Please be seated. Thanks.

Last night I addressed the Nation about our strategy for victory in Iraq and the historic elections that took place in the country last week. In a nation that once lived by the whims of a brutal dictator, the Iraqi people now enjoy constitutionally protected freedoms, and their leaders now derive their powers from the consent of the governed. Millions of Iraqis are looking forward to a future with hope and optimism.

The Iraqi people still face many challenges. This is the first time the Iraqis are forming a Government under their new Constitution. The Iraqi Constitution requires a two-thirds vote of the Parliament for certain top officials, so the formation of the new Government will take time as Iraqis work to build consensus. And once the new Iraqi Government assumes office, Iraq's new leaders will face many important decisions on issues such as security and reconstruction, economic reform, and national unity. The work ahead will require the patience of the Iraqi people and the patience and support of America and our coalition partners.

As I said last night, this election does not mean the end of violence, but it is the beginning of something new, a constitutional democracy at the heart of the Middle East. And we will keep working toward our goal of a democratic Iraq that can govern itself, sustain itself, and defend itself.

Our mission in Iraq is critical to victory in the global war on terror. After our country was attacked on September the 11th and nearly 3,000 lives were lost, I vowed to do everything within my power to bring justice to those who were responsible. I also pledged to the American people to do everything within my power to prevent this from happening again. What we quickly learned was that Al Qaida was not a conventional enemy. Some lived in our cities and communities and communicated from here in America to plot and plan with bin Laden's lieutenants in Afghanistan, Pakistan, and elsewhere. Then they boarded our airplanes and launched the

worst attack on our country in our Nation's history.

This new threat required us to think and act differently. And as the 9/11 Commission pointed out, to prevent this from happening again, we need to connect the dots before the enemy attacks, not after. And we need to recognize that dealing with Al Qaida is not simply a matter of law enforcement; it requires defending the country against an enemy that declared war against the United States of America.

As President and Commander in Chief, I have the constitutional responsibility and the constitutional authority to protect our country. Article II of the Constitution gives me that responsibility and the authority necessary to fulfill it. And after September the 11th, the United States Congress also granted me additional authority to use military force against Al Qaida.

After September the 11th, one question my administration had to answer was how, using the authorities I have, how do we effectively detect enemies hiding in our midst and prevent them from striking us again? We know that a 2-minute phone conversation between somebody linked to Al Qaida here and an operative overseas could lead directly to the loss of thousands of lives. To save American lives, we must be able to act fast and to detect these conversations so we can prevent new attacks.

So, consistent with U.S. law and the Constitution, I authorized the interception of international communications of people with known links to Al Qaida and related terrorist organizations. This program is carefully reviewed approximately every 45 days to ensure it is being used properly. Leaders in the United States Congress have been briefed more than a dozen times on this program. And it has been effective in disrupting the enemy while safeguarding our civil liberties.

This program has targeted those with known links to Al Qaida. I've reauthorized this program more than 30 times since the September the 11th attacks, and I intend to do so for so long as our Nation is—for so long as the Nation faces the continuing threat of an enemy that wants to kill American citizens.

I said the other day that a mistake was trying to train a civilian defense force and an Iraqi Army at the same time but not giving the civilian defense force enough training and tools necessary to be able to battle a group of thugs and killers. And so we adjusted.

And the point I'm trying to make to the American people in this, as you said, candid dialog—I hope I've been candid all along, but in the candid dialog—is to say, we're constantly changing our tactics to meet the changing tactics of an enemy. And that's important for our citizens to understand.

Thank you. Kelly [Kelly Wallace, Cable News Network].

Open Dialog on Wiretaps

Q. Thank you, Mr. President. If you believe that present law needs to be faster, more agile, concerning the surveillance of conversations from someone in the United States to somewhere outside the country—

The President. Right.

Q. —why, in the 4 years since 9/11, has your administration not sought to get changes in the law instead of bypassing it, as some of your critics have said?

The President. No, I appreciate that. First, I want to make clear to the people listening that this program is limited in nature to those that are known Al Qaida ties and/or affiliates. That's important. So it's a program that's limited, and you brought up something that I want to stress, and that is, is that these calls are not intercepted within the country. They are from outside the country to in the country or vice versa. So in other words, this is not a—if you're calling from Houston to L.A., that call is not monitored. And if there was ever any need to monitor, there would be a process to do that.

I think I've got the authority to move forward, Kelly. I mean, this is what it's—and the Attorney General was out briefing this morning and I—about why it's legal to make the decisions I'm making. I can fully understand why Members of Congress are expressing concerns about civil liberties. I know that. And it's—I share the same concerns. I want to make sure the American people understand, however, that we have an obligation

to protect you, and we're doing that and, at the same time, protecting your civil liberties.

Secondly, an open debate about law would say to the enemy, "Here's what we're going to do." And this is an enemy which adjusts. We monitor this program carefully. We have consulted with Members of the Congress over a dozen times. We are constantly reviewing the program. Those of us who review the program have a duty to uphold the laws of the United States, and we take that duty very seriously.

Let's see here—Martha [Martha Raddatz, ABC News]—working my way around the electronic media, here.

Domestic Wiretaps

Q. Thank you, Mr. President. You say you have an obligation to protect us. Then why not monitor those calls between Houston and L.A.? If the threat is so great, and you use the same logic, why not monitor those calls? Americans thought they weren't being spied on in calls overseas—why not within the country, if the threat is so great?

The President. We will, under current law, if we have to. We will monitor those calls. And that's why there is a FISA law. We will apply for the right to do so. And there's a difference—let me finish—there is a difference between detecting, so we can prevent, and monitoring. And it's important to know the distinction between the two.

Q. But preventing is one thing, and you said the FISA laws essentially don't work because of the speed in monitoring calls overseas.

The President. I said we use the FISA courts to monitor calls. It's a very important tool, and we do use it. I just want to make sure we've got all tools at our disposal. This is an enemy which is quick, and it's lethal. And sometimes we have to move very, very quickly. But if there is a need based upon evidence, we will take that evidence to a court in order to be able to monitor calls within the United States.

Who haven't I called on, let's see here. Suzanne [Suzanne Malveaux, Cable News Network].