



SENATE REPUBLICAN

POLICY COMMITTEE

Legislative Notice

No. 43

December 17, 2007

S. 2248 – FISA Amendments Act of 2007

Calendar No. 512

S. 2248 was reported by the Select Committee on Intelligence on October 26, 2007 as an original bill, by a vote of 13-2. S. Rpt. 110-209, with additional and minority views. On November 15, 2007, on sequential referral, the Judiciary Committee recommended a substitute amendment to the bill, and then reported the bill by a vote of 10-9 without a written report.

Noteworthy

- S. 2248 contains language reported by the Intelligence Committee, with a Judiciary Committee substitute as a pending amendment.
- The bill clarifies that FISA's requirement of prior court approval does not apply to surveillance that is targeted at a person reasonably believed to be located outside the United States in accordance with the bill's procedures.
- It provides that the Attorney General (AG) and the Director of National Intelligence (DNI) may jointly authorize the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information for periods of up to one year.
- It reiterates that FISA constitutes the exclusive means by which electronic surveillance and surveillance of domestic communications may be conducted. It also requires prior court approval for surveillance of U.S. citizens who are overseas (the Wyden amendment).
- It provides, upon a certification by the Attorney General, retroactive immunity to carriers that allegedly participated in the President's Terrorist Surveillance Program. It also provides prospective immunity to participating telecommunications carriers for certain assistance.
- The bill's provision for warrantless authority sunsets on December 31, 2013. Among other things, the sunset provision does not apply to the statement of exclusive means.
- The Administration supports S. 2248 as reported by the Intelligence Committee, with some changes, but opposes the Judiciary Committee's substitute amendment.
- On November 15, 2007, the House approved its FISA bill, H.R. 3773, by a vote of 227-189.

Background/Overview

FISA¹ was designed to trace the contours of 4th Amendment protections – establishing procedures for court orders where the Constitution seemed to require it. But rather than focus on the *persons* who could claim Constitutional protection under *Katz v. United States*² and its progeny, FISA focused instead on the technology they used (radio- or wire-communications) and the physical location of the surveillance equipment. It requires prior court approval for activities falling into any one of four categories of “electronic surveillance” – a term defined in Section 101(f) that in effect defines the scope of FISA.

Because the underlying technology was evolving fast, with no end in sight, there was little chance that the factors defining FISA’s coverage would remain stable. For this reason, the meaning of “electronic surveillance” as defined in FISA – and therefore the scope of the statute itself – has drifted with technological change since 1978. In particular, the distinction that existed between radio and wire communications in 1978, critical to ensuring that FISA would operate as intended, has been lost with the modern revolution in telecommunications. Most international and domestic telecommunication nowadays are a seamless mix of both radio and wire communications.

After it was revealed that the attacks of September 11, 2001 had depended on extensive “wire communications” of known terrorist suspects outside the United States, the President instituted what came to be known as the Terrorist Surveillance Program (TSP). The administration based the TSP on the President’s inherent constitutional authority to conduct wartime surveillance of foreign enemies outside the United States.

The existence of the TSP was revealed in December 2005, triggering great controversy. The controversy had not been resolved a year later when the Attorney General announced in a January 17, 2007 letter to Congress that a judge of the FISA Court had authorized the surveillance contemplated in the TSP “where there is probable cause to believe one of the communicants is a member or agent of al Qaeda or an associated terrorist group” and that such surveillance would now be conducted subject to FISA Court approval.

On April 12, 2007, in response to a congressional request, the DNI submitted a legislative proposal that would address the intelligence challenges arising under FISA in a manner consistent with the Constitution. The DNI’s proposal was a comprehensive reform aimed at making the scope of FISA technology-neutral and therefore stable in its meaning.

While this proposal was being considered, it became known at the end of May 2007 that another judge of the FISA Court had issued a ruling which, according to the DNI, severely limited collection of critical communications of foreign terrorists and diverted NSA analysts

¹ In its original version FISA provided both immunity to telecommunications carriers that were required to assist the government, and – in certain cases specifically *excluding* terrorists – a procedure and authority for warrantless surveillance.

² 389 U.S. 347 (overruling *Olmstead v. United States*, 277 U.S. 438).

from their counterterrorism mission to providing information to the Court, thus degrading the government's counterterrorism capabilities.

The DNI urged Congress to act quickly, and on August 4, 2007, it passed the Protect America Act of 2007 (PAA), which grants the AG and DNI authority to acquire foreign intelligence information concerning persons outside the United States for one year. The PAA sunsets February 1, 2008.

On October 26, the Select Committee on Intelligence (SSCI) reported S. 2248. The SSCI chose not to fix the inherent problems in FISA by making its definition of "electronic surveillance" technology-neutral, electing instead to carve out of the old definition of "electronic surveillance" any surveillance targeted at persons reasonably believed to be outside the United States, and providing a warrantless procedure for such surveillance. The procedures also require FISA Court approval of collection on U.S. persons overseas for the first time in history (the Wyden amendment). The SSCI bill also provides retroactive and prospective immunity from civil suits to certain telecommunications carriers.

The Senate Judiciary Committee subsequently took up the legislation, and on November 15, 2007, voted 10-9 to report a substitute amendment that does not address carrier liability and would significantly alters the government's ability to conduct surveillance of foreign enemies. If adopted, the amendment would incur a veto-threat from the administration.

Highlights

S. 2248 contains three titles:

- Title I includes, in section 101, a new Title VII of FISA that provides a procedure for the DNI and AG jointly to authorize surveillance targeted at persons reasonably believed to be located outside the United States. It is a successor to the Protect America Act and sunsets after six years. Section 102 contains a statement that FISA is the exclusive means for electronic surveillance. Section 103 provides for reports to Congress. Sections 104 to 110 streamline FISA procedures and contain certain technical amendments to FISA.
- Title II, "Protections for Electronic Communication Service Providers," provides, in Section 202, retroactive immunity from civil suits involving intelligence activity authorized by the president under the Terrorist Surveillance Program between September 11, 2001 and January 17, 2007. Section 203 provides prospective immunity for carriers who cooperate with the intelligence community pursuant to strictly defined requests. Section 204 preempts state investigations of the federal government's intelligence collection activities under FISA.
- Title III provides for the transition from the Protect America Act to the new Title VII of FISA, as well as authority for the government to continue to apply to the FISA Court for orders under Title I of FISA as it had in the past. It also provides for continuance of

activities authorized under the new FISA Title VII before the December 31, 2013 sunset, until their expiration within the year following the sunset.

Bill Provisions

Section 1. Short Title; Table of Contents

TITLE I—FOREIGN INTELLIGENCE SURVEILLANCE

Section 101. Targeting the communications of certain persons outside the United States.

Consists of three subsections:

(a) In General. This section amends FISA by adding a new Title VII.³ The new FISA title VII consists of four sections:

Section 701. Limitation on Definition of Electronic Surveillance. This section clarifies some of the ambiguity that has crept into the FISA categories of “electronic surveillance” with the changes in communications technology since 1978. It removes from the requirements of Title I court warrants, which apply to “electronic surveillance” as defined in Title I, surveillance targeted at persons reasonably believed to be outside the U.S. in accordance with the procedures of Title VII.

Section 702. Definitions. This section defines “Electronic Communications Service Provider,” among other terms.

Section 703. Procedures for Acquiring the Communications of Certain Persons outside the United States. A central provision of S. 2248, this section provides a procedure whereby the Attorney General (AG) and Director of National Intelligence (DNI) may jointly authorize the targeting of persons reasonably believed to be located outside the United States for up to one year without prior court approval to acquire foreign intelligence information. The provision has twelve subsections:

(a) Authorization—creates the authority.

(b) Limitations—provides several safeguarding limitations. The authority cannot be used to target any person:

- “known at the time” to be located in the U.S.;

³ Because communications may be acquired both during live transmission and while they are stored on physical media, circumstances that correspond to two separate titles of FISA (Titles I and III, respectively), the authority provided by this bill is set forth in a title of its own – a new Title VII. The new title replaces a Title VII consisting of technical provisions unrelated to the subject matter of the present act.

- who is outside the U.S. if the purpose is to target a “particular, known person” in the U.S. (so-called “reverse targeting”); or
- in any manner inconsistent with the 4th Amendment to the Constitution.

(c) *United States Persons Located Outside the United States*—permits acquisitions *outside* the U.S. of the communications of U.S. persons outside the U.S. only on a FISA Court finding of probable cause that the person is a foreign power or agent of a foreign power.⁴

(d) *Conduct of Acquisition*—requires that any acquisition authorized under subsection (a) be certified under subsection (g) and comply with the procedural safeguards provided in subsections (e) and (f).

(e) *Targeting Procedures*—requires special procedures to ensure that targeted persons are located outside the U.S. subject to judicial review under subsection (i).

(f) *Minimization Procedures*—requires the AG to adopt “minimization procedures” and makes the procedures subject to judicial review. The term “minimization procedures” refers to a series of procedures governing the acquisition, retention, or dissemination of information pertaining to U.S. persons, consistent with the need to disseminate foreign intelligence information.⁵

(g) *Certification*—Specifies that before the § 703(a) authority may be exercised, the AG and DNI must certify that:

- the targeting and minimization procedures to be used have been approved or will be submitted to the Foreign Intelligence Surveillance Court (FISC) for approval;
- the acquisition will comply with the 4th Amendment to the Constitution;
- that a significant purpose of the acquisition is to obtain foreign intelligence information;
- the minimization procedures to be used meet the definition under section 101(h) of FISA; and
- that an electronic communications service provider is participating in the acquisition.

⁴ This provision codifies a similar provision of President Reagan’s Executive Order 12333 of December 4, 1981. Acquisitions that occur *inside* the U.S. of U.S. persons located outside the U.S. constitute “electronic surveillance” under FISA Title I; the requirement of prior court approval in such situations is unaffected by S. 2248.

⁵ Most existing “minimization procedures” have been mandatory within the intelligence community for decades pursuant to applicable directives. The procedures are designed to protect the identity and other private information of U.S. persons that is not foreign intelligence information.

(h) *Directives*—empowers the AG and DNI to require electronic communication service providers to provide the information authorized for collection under Title VII. This subsection also provides for recourse to the FISA courts for enjoining (or enforcing) the directives.

(i) *Judicial review*—provides extensive procedures for judicial review of the implementation of Title VII.

(j) *Judicial proceedings*—sets forth procedural provisions.

(k) *Maintenance of records*—provides record-keeping for documents and proceedings under Title VII, including statements of reasons for decisions of the FISA courts thereunder.

(l) *Oversight*—provides for extensive review, oversight, and reporting by the Department of Justice, the Director of National Intelligence, and agency heads, as well as review and oversight by the FISC and Congress.

Section 704. Use of information acquired under Section 703. This section makes public disclosure and use in criminal proceedings of the information acquired pursuant to Title VII subject to the same provisions as specified in Title I, except for the provision in subsection (j) relating to notice following emergency authorization.

(b) Table of Contents.

(c) Sunset. Provides that the new Title VII sunsets December 31, 2013.

Section 102. Statement of exclusive means by which electronic surveillance and interception of domestic communications may be conducted. This section reiterates current law that FISA is the exclusive means by which “electronic surveillance”⁶ and interception of domestic wire, oral, or electronic communications may be conducted. Unlike Title VII, this provision does not sunset in 2013.

Section 103. Submittal to Congress of certain court orders under the Foreign Intelligence Surveillance Act of 1978. This section expands reporting to Congress by requiring copies of FISC court orders, decisions, and opinions that contain a significant interpretation of FISA to be provided on a new accelerated timetable.

Sections 104 through 108. FISA Streamlining. These largely technical provisions are meant to increase the speed and efficiency of the FISA process, by:

- updating certain technologically obsolete provisions;

⁶ As defined in FISA Section 101(f), “regardless of the limitation of section 701.”

- reducing paperwork;
- modifying time requirements, including extending emergency authorization from 72 to 168 hours; and
- expanding the pool of officials who can authorize FISA actions, including the Deputy Director of the FBI.

Section 109. Foreign Intelligence Surveillance Court. This section streamlines Section 103 of FISA, which establishes the FISA Court and Court of Review, by

- relaxing one of the restrictions on the composition of the FISA Court;
- making it easier to have hearings and rehearings of the FISA Court sitting *en banc* (the full court rather than just one judge); and
- providing some flexibility during the pendency of proceedings in the Supreme Court.

Section 110. Technical and conforming amendments.

TITLE II—PROTECTIONS FOR ELECTRONIC COMMUNICATION SERVICE PROVIDERS

This title provides immunity to electronic communication service providers who allegedly provided assistance to the government under the Terrorist Surveillance Program until its termination on January 17, 2007 (Sections 201 and 202) and under FISA (Sections 203 and 204). Because Sections 201 and 202 cover situations that occurred in the past and outside the scope of FISA, they do not amend FISA. Sections 203 and 204, on the other hand, do cover FISA activities and create a new FISA Title VIII (Sections 801 to 803).

Section 201. Definitions. This section defines, among other terms, the scope of civil actions covered by the Section 202 immunity: “covered civil actions” are those which seek monetary damages against service providers for providing certain assistance to the intelligence community.

Section 202. Limitations on civil actions for electronic communication service providers. This provides retroactive immunity from “covered civil actions” if a series of conditions are met:

- the assistance was provided in connection with intelligence activity (1) authorized by the President between September 11, 2001 and January 17, 2007, and (2) designed to detect or prevent a terrorist attack against the U.S.; and
- the assistance was provided in response to a written request or directive from the AG or other intelligence community head indicating that the activity had been (1) authorized by the President and (2) determined to be legal.

Sections 203 and 204. Procedures for implementing statutory defenses under the Foreign Intelligence Surveillance Act of 1978; Preemption of state investigations. These sections create a new FISA Title VIII composed of the following:

Section 801. Definitions.

Section 802. Procedures for Implementing Statutory Defenses—Requires for immunity an AG certification to the effect that either the service was not provided or that it was provided pursuant to one of several specified statutory requirements.

Section 803. Preemption of State Investigations.

Section 205. Technical amendments.

TITLE III—OTHER PROVISIONS

Section 301. Severability.

Section 302. Effective date; repeal; transition procedures.

Administration Position

In a Statement of Administration Policy released today, the White House expressed its support for the Intelligence Committee’s version of S. 2248, stating: “Although the bill is not perfect and its flaws must be addressed, it nevertheless represents a bipartisan compromise that will ensure that the Intelligence Community retains the authority it needs to protect the Nation.”

By contrast, the White House expressed strong opposition to the Judiciary Committee substitute, saying that it “would have devastating consequences to the Intelligence Community’s ability to detect and prevent terrorist attacks and to protect the Nation from other national security threats.” The White House elaborated:

“The Judiciary Committee proposal would degrade our foreign intelligence collection capabilities. The Judiciary Committee’s amendment would impose unacceptable and potentially crippling burdens on the collection of foreign intelligence information by expanding FISA to restrict facets of foreign intelligence collection never intended to be covered under the statute. Furthermore, the Judiciary Committee amendment altogether fails to address the critical issue of liability protection. Accordingly, if the Judiciary Committee’s substitute amendment is part of a bill that is presented to the President, the Director of National Intelligence, the Attorney General, and the President’s other senior advisors will recommend that he veto the bill.”

Possible Amendments

As of the publication of this notice, there is no unanimous consent agreement that limits the submission of amendments.

A managers' amendment is being negotiated to fix two provisions adopted in the Intelligence Committee's markup: the provision relating to prior FISC approval for surveillance of U.S. persons overseas (the Wyden amendment) and an element of the reporting requirements relating to the IG and annual reviews, both of which in their current versions would produce negative unintended consequences. Senators Rockefeller and/or Bond may introduce a version of the Intelligence Committee's bill that contains the two perfecting fixes currently under negotiation.

The Judiciary Committee markup of the bill is a pending substitute amendment. It provides a more limited warrantless procedure for surveillance of non-U.S. persons outside the United States, with more stringent oversight and reporting requirements, and does not provide any relief to telecommunications carriers facing civil lawsuits for their cooperation with the government's warrantless surveillance activities. It differs from the Intelligence Committee's bill on a number of issues, including the following:

- Retroactive immunity;
- Exclusive means;
- Stay pending appeal;
- Use of foreign intelligence information;
- Reverse targeting prohibition;
- Bulk collection prohibition;
- FISC assessing compliance;
- Inspector General audit; and
- Sunset.

On any of the above issues, the Judiciary Committee language could be presented as an individual amendment. In particular, it is expected that various amendments will be offered to address the issue of carrier liability, including proposals that would provide government indemnity of any liability incurred by participating carriers, and proposals that would substitute the U.S. government for the carriers in relevant lawsuits.