NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 85072A
27 September 2016

JOHN GREENEWALD
[redacted]

Dear Mr. Greenewald:

This responds to your Freedom of Information Act (FOIA) request of 23 July 2016 for "Copy of the Intellipedia entry (from all three Wikis that make up the Intellipedia) for the following entry(s) (Or whatever similar topic may pertain if it is slightly worded differently): Foreign Intelligence Surveillance Act and/or FISA and/or Foreign Intelligence Surveillance Act of 1978 and/or Terrorist Surveillance Act and/or Terrorist Surveillance Act of 2006 and/or Protect America Act of 2007 and/or Protect America Act, and the search results page." As stated in our initial response letter, dated 26 July 2016, your request was assigned Case Number 85072. For purposes of this request and based on the information you provided in your letter, you are considered an "all other" requester. As such, you are allowed 2 hours of search and the duplication of 100 pages at no cost. There are no assessable fees for this request. A copy of your request is enclosed. Your request has been processed under the FOIA.

For your information, NSA provides a service of common concern for the Intelligence Community (IC) by serving as the executive agent for Intelink. As such, NSA provides technical services that enable users to access and share information with peers and stakeholders across the IC and DoD. Intellipedia pages are living documents that may be originated by any user organization, and any user organization may contribute to or edit pages after their origination. Intellipedia pages should not be considered the final, coordinated position of the IC on any particular subject. The views and opinions of authors do not necessarily state or reflect those of the U.S. Government.

We conducted a search of all three levels of Intellipedia for the requested topics, and located four documents that are responsive to your request. The documents are enclosed. Certain information, however, has been deleted from the enclosures.

This Agency is authorized by statute to protect certain information concerning its activities (in this case, internal URLs) as well as the names of its employees. Such information is exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statute applicable in this case is Section 6, Public Law 86-36 (50 U.S. Code 3605). We have determined that such information exists in this record, and we have excised it accordingly.

In addition, personal information regarding individuals has been deleted from the enclosures in accordance with 5 U.S.C. 552 (b)(6). This exemption protects from disclosure information that would constitute a clearly unwarranted invasion of personal privacy. In balancing the public interest for the information you request against the privacy interests involved, we have determined that the privacy interests sufficiently satisfy the requirements for the application of the (b)(6) exemption

Since these deletions may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures. You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below.

- The appeal must be in writing and addressed to:

  NSA/CSS FOIA/PA Appeal Authority (P132),
  National Security Agency
  9800 Savage Road STE 6932
  Fort George G. Meade, MD 20755-6932

- It must be postmarked no later than 90 calendar days of the date of this letter.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of the requested information was unwarranted.
- NSA will endeavor to respond within 20 working days of receiving your appeal, absent any unusual circumstances.

Sincerely,

Paul K
for

JOHN R. CHAPMAN
Chief, FOIA/PA Office
NSA Initial Denial Authority

Encls:
a/s

From: donotreply@nsa.gov
Sent: Saturday, July 23, 2016 6:50 PM
To: donotreply@nsa.gov
Subject: FOIA Request (Web form submission)

Title: Mr.

Full Name: John Greenewald

email: john@greenewald.com

Company: The Black Vault

Postal Address: [redacted]

Postal City: [redacted]

Postal State-prov: [redacted]

Zip Code: [redacted]

Country: United States of America

Home Phone: [redacted]

Work Phone: [redacted]

Records Requested: To whom it may concern,

This is a non-commercial request made under the provisions of the Freedom of Information Act 5 U.S.C. S 552. My FOIA requester status as a "representative of the news media" however due to your agency's denial of this status, I hereby submit this request as an "All other" requester.

I prefer electronic delivery of the requested material either via email to john@greenewald.com or via CD-ROM or DVD via postal mail. Please contact me should this FOIA request should incur a charge.

I respectfully request a copy of the Intellipedia entry (from all three Wikis that make up the Intellipedia) for the following entry(s) (Or whatever similar topic may pertain if it is slightly worded differently):

Foreign Intelligence Surveillance Act

and/or

FISA

and/or

Foreign Intelligence Surveillance Act of 1978

and/or

Terrorist Surveillance Act

and/or

Terrorist Surveillance Act of 2006

and/or

Protect America Act of 2007

and/or

Protect America Act

I also ask that you include a copy of the search results page, when inserting the above words / phrases into the Intellipedia search engine.

Thank you so much for your time, and I am very much looking forward to your response.

Sincerely,

John Greenewald, Jr.
[redacted]

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

(U) Protect America Act

UNCLASSIFIED

From Intellipedia

You have new messages (last change).

(U) Be bold in modifying this **Wikipedia** import .

(U) Correct mistakes; remove bias; categorize; delete superfluous links, templates, and passages; add classified information and citations.

(U) When assimilation into Intellipedia is complete, remove this template and add {{From Wikipedia}}.

The **Protect America Act of 2007** (**PAA**) is an amendment to the Foreign Intelligence Surveillance Act (FISA) that was signed into law on August 5, 2007. It removed the warrant requirement for government surveillance of foreign intelligence targets "reasonably believed" to be outside of the United States. [1] Due to a sunset clause the law expired on February 17, 2008.

Contents

- 1 Background
- 2 Changes made to prior law
  - 2.1 Warrant and notification requirements
  - 2.2 Domestic wiretapping
  - 2.3 Foreign wiretapping
  - 2.4 Data monitoring
  - 2.5 Authorization power
  - 2.6 Reporting requirements
- 3 Legislative history
  - 3.1 Amendments
- 4 See also
- 5 References
- 6 External links

Background

Main article: NSA warrantless surveillance controversy

In December 2005, the *New York Times* published an article[2] that described a surveillance program of warrantless domestic wiretapping ordered by the Bush administration and carried out by the National Security

Agency in cooperation with major telecommunications companies since 2002 (a subsequent Bloomberg article[3] suggested that this may have already begun by June 2000). Many critics have asserted that the Administration's warrant-free surveillance program is a violation of the Fourth Amendment to the United States Constitution against warrantless search, and, a criminal violation of FISA.

The Bush administration maintained that the warrant requirements of FISA were implicitly superseded by the subsequent passage of the Authorization for Use of Military Force Against Terrorists.[4], and that the President's inherent authority under Article II of the Constitution to conduct foreign surveillance trumped the FISA statute. However, the Supreme Court decision in *Hamdan v. Rumsfeld* placed the legitimacy of this argument into question.[5][6]

On July 28, 2007, President Bush announced that his Administration had submitted a bill to Congress to amend FISA. He suggested that the current law was "badly out of date" - despite amendments passed in October 2001 - and did not apply to disposable cell phones and Internet-based communications. The bill he submitted to Congress would address these new technologies, Bush said, as well as restore FISA's "original focus" on protecting the privacy of people within the United States, "so we don't have to obtain court orders to effectively collect foreign intelligence about foreign targets located in foreign locations." [2] (http://www.whitehouse.gov /news/releases/2007/07/20070728. html) He asked that Congress pass the legislation before its August 2007 recess, stating that "Every day that Congress puts off these reforms increases the danger to our nation. Our intelligence community warns that under the current statute, we are missing a significant amount of foreign intelligence that we should be collecting to protect our country."

On August 3, 2007, the Senate passed the Republican-sponsored bill (S. 1927 (http://www.opencongress.org /bill/110-s1927/show)) in a vote of 60 to 28(110th Congress 1st Session Vote 309 (http://www.senate.gov /legislative/LIS/roll_call_lists /roll_call_vote_cfm.cfm?congress=11 0&session=1&vote=00309)). The House followed by passing the bill, 227-183(House Roll Call 836 (http://clerk.house.gov/evs/2007 /roll836.xml)) on August 4, 2007.

Changes made to prior law

The bill altered the original 1978 law in many ways, including:[7]

Warrant and notification requirements

The bill amended FISA to substitute the requirement of a warrant to conduct surveillance with a system of NSA (National Security Agency) internal controls.[7]

The bill required notification to the FISA Court of warrantless surveillance within 72 hours of any authorization. The bill also required that "a sealed copy of the certification" be sent which would "remain sealed unless the certification is needed to determine the legality of the acquisition."[7]

Domestic wiretapping

The bill allowed the monitoring of electronic communications on people "reasonably believed to be outside the United States," without a court's order or oversight. It continues to require a court order to conduct electronic surveillance or physical search when targeting persons located in the United States. [1] [8]

Foreign wiretapping

The bill clarified confusion in current law by allowing the National Security Agency to collect purely foreign communications in the future without a warrant.[8]

Data monitoring

In the bill, the monitoring of data related to Americans communicating with foreigners who are the targets of a U.S. terrorism investigation was addressed. This data could be monitored only if intelligence officials have a reasonable expectation of learning information relevant to that probe.[8]

Authorization power

Under the bill, the director of national intelligence and the attorney general could authorize the surveillance of all communications involving foreign targets. The Foreign Intelligence Surveillance Court, composed of federal judges whose deliberations are secret, could only examine whether the government's guidelines for targeting overseas suspects are appropriate.[7]

The guidelines for authorizing surveillance were:

- There was reason to believe that the target of the acquisition was outside the U.S. and that the procedures used would be subject to the review of the FISA Court.
- That the acquisition involved obtaining the foreign intelligence with the assistance of a telecommunications service provider or other persons who would have access to communications, either as they were transmitted or while they were stored, or access to equipment being used to transmit or store the communications.
- That the significant purpose of the procedure would be to acquire foreign intelligence information.

The certification of the determination (sent to the Court) would be written, signed under oath and supported by affidavit of security officials appointed by the president and confirmed by the Senate, or the head of any intelligence community agency.[7]

If the determination required immediate action and time would not permit preparing a certification, the certification supporting the determination would be submitted in writing to the Court no more than 72 hours after it was made. The AG would transmit as soon as possible to the Court a sealed copy of the certification that would remain sealed unless the certification was needed to determine the legality of the acquisition.[7]

Reporting requirements

The Attorney General would report to Congress semi-annually with:

- A description of any incidents of non-compliance with a directive issued.[7]
- Incidents of non-compliance with the guidelines or procedures established for determining that the acquisition concerns persons outside the United States by any entity of the Intelligence Community.[7]
- Incidents of noncompliance by a specified person to whom the Attorney General and Director of National Intelligence issued a directive.[7]
- The number of certifications and directives issued in the preceding six months.[7]

Legislative history

Senator Mitch McConnell introduced the act on August 1, 2007, during the 110th United States Congress. On August 3, it was passed in the Senate with an amendment, 60-28 (record vote number 309).[9] On August 4, it passed the House of Representatives 227-183 (roll number 836).[9] On August 5, it was signed by President Bush, becoming Public Law No. 110-055. On February 17, 2008, it expired due to sunset provision.

Amendments

Template:USBill provides a sunset provision. The sunset provision was passed due to concerns of many members of Congress about the long-term effects of the legislation. Some scholars believe that any future extension of the act will be less expansive than the current time-limited version. [3] (http://www.cyberlawonline. com/cyberlawg/privacy/pr otect-america-act-of-2007.html)

See also

- USA PATRIOT Act
- Communications Assistance for Law Enforcement Act (CALEA)
- War on Terror
- Legal challenges to NSA warrantless searches in the United States
- Total information awareness
- Intelligence Community Oversight Discussion

References

1. ↑ 1.0 1.1 Statement for the Record to the House Judiciary Committee by Director John Michael McConnell September 18, 2007
2. ↑ "Bush Lets US Spy on Callers Without Courts" (Dec. 16, 2005; [1] (http://www.commondreams.org /headlines05/1216-01.htm)
3. ↑ Bloomberg.com: Worldwide (http:// www.bloomberg.com/apps/news?pid= 20601087& sid=abIV0cO64zJE&refer=)
4. ↑ U.S. Department of Justice White Paper on NSA Legal Authorities "Legal Authorities Supporting the Activities of the National Security Agency Described by the President" January 19 2006.
5. ↑ Supreme Court's Ruling in Hamdan Means Warrantless Eavesdropping is Clearly Illegal (http://www.crooksandliars.com/ 2006/07/09/supreme-courts-ruling -in-hamdan-means-warrantless-eavesdropping-is-clearly-illegal /) , Glenn Greenwald, July 9, 2006
6. ↑ Hamdan and the NSA Domestic Surveillance Program: What Next? (http://balkin.blogspot.com /2006/07/hamdan-and-nsa-domesti c-surveillance.html) , Marty Lederman, July 7, 2006
7. ↑ 7.0 7.1 7.2 7.3 7.4 7.5 7.6 7.7 7.8 7.9 GovTrack U.S. – S. 1927 Text of Legislation (http://www.govtrack.us /congress/billtext.xpd?bill=s110 -1927)
8. ↑ 8.0 8.1 8.2 Nakashima, Ellen; Warrick, Joby (2007-08-05). House Approves Wiretap Measure (http://www.washingtonpost.com/ wp-dyn/content/article/2007/08 /04/AR2007080400285.html?nav=rss _politics) . Washington Post. Retrieved on 2007-08-10.
9. ↑ 9.0 9.1 GovTrack U.S. – S. 1927 (http://www.govtrack.us/congress/bill.xpd?b ill=s110-1927)

DOCID: 4321853

(U) {FISA}

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

External links

- Department of Justice's Support for the Protect America Act (http://www.dotgovwatch.com/?/archives /17-Department-of-Ju stice-Website-Illegally-Lobbies -Congress-LifeAndLiberty.gov.htm l)
- GovTrack U.S. – S. 1927 (http://www.govtrack.us/congress/bill.xpd?b ill=s110-1927)
- Congresspedia – S. 1927 (http://www.sourcewatch.org /index.php?title=U.S._congressio nal_action_on_domestic_wiretapping)
- Plural Politics Protect American Act Plainspeak Legal Primer (http://eteraz.org/2007/ 08/11/short-primer-on-new-fisa/)

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

Retrieved from

Categories: Privacy | Terrorism laws | Emergency laws | Espionage | United States federal defense and national security legislation | 2007 in the United States

UNCLASSIFIED

- This page has been accessed 1,174 times.
- 2 watching users (b)(6)
- This page was last modified 16:13, 17 January 2011 by Most recent editors: and

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

c2linipedweb2j

(U) Foreign Intelligence Surveillance Act

UNCLASSIFIED

From Intellipedia

The **Foreign Intelligence Surveillance Act (FISA)** establishes a legal regime for "foreign intelligence" surveillance separate from ordinary law enforcement surveillance. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95- 511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-1811, 1821-1829, 1841-1846, 1861-62).

Contents

- 1 Purpose
- 2 History
- 3 Procedures
- 4 Definitions
- 5 Constitutionality

Purpose

FISA is aimed at regulating the collection of "foreign intelligence" information in furtherance of U.S. counterintelligence, whether or not any laws were or will be broken. *Counterintelligence* is defined in 50 U.S.C. § 401(a)(3) as information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Department of Defense (DOD) guidelines state that the purpose of counterintelligence collection is to detect espionage, sabotage, terrorism, and related hostile intelligence activities to "deter, to neutralize, or to exploit them." In short, counterintelligence and criminal prosecution are different.

Given the "tendency of those who execute the criminal laws ... to obtain conviction by means of unlawful seizures," the Supreme Court has viewed communications interception as an especially grave intrusion on rights of privacy and speech. Berger v. New York, 388 U.S. 41, 50 (1967) (quotation and citation omitted). "By its very nature eavesdropping involves an intrusion on privacy that is broad in scope," and its "indiscriminate use . . . in law enforcement raises grave constitutional questions." Id. at 56 (quotation and citation omitted). "Few threats to liberty exist which are greater than those posed by the use of eavesdropping devices." Id. at 63.

Thus, the Court outlined seven constitutional requirements:

1. a showing of probable cause that a particular offense has been or is about to be committed;
2. the applicant must describe with particularity the conversations to be intercepted;
3. the surveillance must be for a specific, limited period of time in order to minimize the invasion of privacy (the N.Y. law authorized two months of surveillance at a time);
4. there must be continuing probable cause showings for the surveillance to continue beyond the original termination date;
5. the surveillance must end once the conversation sought is seized;

6. notice must be given unless there is an adequate showing of exigency; and
7. a return on the warrant is required so that the court may oversee and limit the use of the intercepted conversations.

Indeed, the Court said that if "neither a warrant nor a statute authorizing eavesdropping can be drawn so as to meet the Fourth Amendment's requirements ... then the "fruits" of eavesdropping devices are barred under the Amendment." Id., at 63.

Where intelligence operations are concerned, however, the bounds of the Fourth Amendment are less clear than they are for ordinary criminal investigations. FISA creates a special court and legal regime for counterintelligence surveillance orders.

Executive Order 12,333 File:Executive Order 12333.doc (1981) provides the general framework for U.S. intelligence activities, and it also addresses electronic surveillance. "[A]gencies are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General." EO 12,333, para. 2.4. Dep't. of Defense (DOD) Directive 5240.1-R implements FISA and EO 12,333 within DOD. These authorities govern the collection of intelligence by the U.S. government against United States persons, whether they are located within the United States or outside the United States.

FISA does not regulate the use of electronic surveillance outside of the United States. For instance, electronic surveillance of electronic communications like e-mail is only governed by §1801(f)(4) if the surveillance device is installed "in the United States." When e-mail sent by a U.S. person to a foreign person is intercepted outside the United States, that interception does not meet this definition.

History

The path to FISA has two branches, political and judicial. The government had long maintained that it had extensive discretion to conduct wiretapping or physical searches in order to protect national security. In *Katz v. United States*, 389 U.S. 347 (1967), the Supreme Court acknowledged that the President had claimed special authority for warrantless surveillance in national security investigations, and explicitly declined to extend its holding to cases "involving the national security." Id. at 358 n. 23. Similarly, Congress in Title III stated that "nothing in Title III shall ... be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government."

On the political front, such executive branch activities, charitably described as "some degree of domestic overreaching of intelligence into domestic areas," had long been tolerated. Staff of House Permanent Select Comm. on Intelligence, 104th Cong., Staff Study, *IC21: Intelligence Community in the 21st Century* at 272 (comm. print 1996).

But in the 1970s the political winds changed. The 1975-76 Church Committee hearings documented extraordinary federal government abuse of surveillance powers. Examples included the the NSA's Operation Shamrock and Operation Minaret, CIA's Operation CHAOS, the FBI's COINTELPRO domestic harassment of dissenters and anti-war protesters that included illegal wiretapping, and the

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

illegal burglaries of the Nixon White House "plumbers."

The Church Committee Report found that covert action had been excessive, had circumvented the democratic process, and had violated the Constitution. It concluded that Congress needed to prescribe rules for intelligence activities.

On the judicial front, the Supreme Court first confronted the tension between unmonitored executive branch surveillance and civil liberties in United States v. U.S. District Court, 407 U.S. 297 (1972), in which the United States charged defendants with conspiracy to destroy government property. Defendants sought electronic surveillance information, held by the prosecution, that the CIA obtained during a potentially illegal wiretap, wanting to ascertain whether the government had relied on information in the indictment or the case for conviction and to suppress any tainted evidence at trial. The Attorney General admitted that a warrantless wiretap had intercepted conversations involving the defendants.

Before the Supreme Court, the government defended its actions on the basis of the Constitution and the Title III national security disclaimer. The Court rejected the statutory argument, saying that "Congress ... simply did not legislate with respect to national security surveillances." As for the constitutional argument, the Court accepted that the President had the power "to protect our Government against those who would subvert or overthrow it by unlawful means" and that this power justified electronic surveillance of would-be subversives.

Invoking the "broader spirit" of the Fourth Amendment and "the convergence of First and Fourth Amendment values" in national security wiretapping cases, however, the Court was especially wary of possible abuses of the national security power. The Court then balanced "the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression," and found that waiving the Fourth Amendment probable cause requirement could lead the executive to "yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech." Justice Powell wrote that the inconvenience to the government is "justified in a free society to protect constitutional values."

The Court emphasized that this case involved only the domestic aspects of national security: "We ... express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents." It invited Congress to act: "Given these potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens." These two paths, political and judicial, converged in the enactment of FISA.

Procedures

Under current law, any FISA investigation must have FII collection as its "primary purpose." Crossing the "primary purpose" line for information collection (from counterintelligence to law enforcement) subjects the investigation and evidence to extensive legal scrutiny and policy concerns. For instance, under DOD Dir. 5240.1-R, procedure 1, A, 3, DOD components cannot use the procedures for collecting intelligence information as a subterfuge for collecting evidence for a prosecutorial purpose. This would

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

change under draft Anti-Terrorism Act of 2001 (ATA).

FISA established a special court, composed of seven federal district court judges appointed by the Chief Justice for staggered terms and are from different circuits. See 50 U.S.C.A. § 1803. Individual judges of the FISC review the Attorney General's applications for authorization of electronic surveillance aimed at obtaining foreign intelligence information. The proceedings are nonadversarial and are based solely on the DOJ's presentations through its Office of Intelligence Policy and Review.

The records and files of the cases are sealed and may not be revealed even to persons whose prosecutions are based on evidence obtained under FISA warrants, except to a limited degree set by district judges' rulings on motions to suppress. 50 U.S.C. §1803(c). There is no provision for the return of each executed warrant to the FISC, much less with an inventory of items taken, nor for certification that the surveillance was conducted according to the warrant and its "minimization" requirements.

The FISC meets two days monthly, and two of the judges are routinely available in the Washington, D.C. area on other days. Statement of Mary C. Lawton, Counsel for Intelligence Policy, Before the House Subcommittee on Courts, Civil Liberties, and the Administration of Justice, June 8, 1983, at 8.

Originally, FISA was limited to electronic eavesdropping and wiretapping. 50 U.S.C. § 1801(f). In 1994 it was expanded to permit covert physical entries in connection with "security" investigations. 50 U.S.C. §§ 1821-1829. In 1998, it was amended to permit pen/trap orders, 50 U.S.C. §§ 1841-1846. FISA can also be used to obtain certain business records. §§ 1861-62.

Definitions

Although orders issued under FISA are sometimes called FISA "warrants," this is misleading because it suggests that the FISA order is like an ordinary search warrant or Title III intercept order, which it is not. Under the Fourth Amendment, a search warrant must be based on probable cause to believe that a crime has been or is being committed. This is not the general rule under FISA.

Under FISA, surveillance is generally permitted based on a finding of probable cause that the surveillance target is a foreign power or an agent of a foreign power -- not whether criminality is in any way involved. §1801(b)(1).

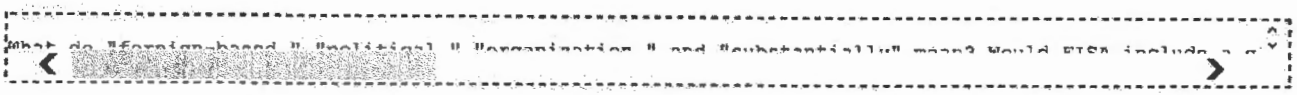
Examples of groups that would likely meet the definition of "foreign power" are the Irish Republican Army, Hezbollah, the PFLP, the ANC, and the FMLN. Note that a "foreign power" need not engage in activities hostile to U.S. interests.

A "foreign power" is

- a foreign government or a component thereof, whether or not recognized by the United States, 50 U.S.C. § 1801(a)(1)
- a "faction" of a foreign nation or nations, not substantially composed of United States persons, 50 U.S.C. § 1801(a)(2). The term "substantially" is not defined.
- any entity that a foreign government acknowledges it controls and directs, such as government trading or business corporations, § 1801(a)(3). It is unclear whether general regulation of a foreign corporation constitutes control and direction.
- any entity that in fact is controlled and directed by a foreign government. § 1801(a)(6). Given

FISA's structure, it appears that this is decided by the FISA court.

- any group engaged in international terrorism or "activities in preparation therefor," not only governments or their components. § 1801(a)(4).
- any "foreign-based political organization, not substantially composed of United States persons." § 1801(a)(5).



What is an "agent of a foreign power"? FISA §1801(b) defines this phrase in two ways, depending on whether the target is a U.S. person. §1801(b)(1) covers non-U.S. persons, while § 1801(b)(2) covers "any person."

Non-U.S. persons are "agents" under FISA if they

- act in the United States as an officer or employee of a foreign power, or as a member of a terrorist organization, § 1801(b)(1)(A)
- act for or on behalf of a foreign power that engages in clandestine intelligence activities in the United States contrary to U.S. interests when
  1. the circumstances of such persons' presence in the United States "indicate that such person may engage in such activities, or
  2. when such person knowingly aids or abets any person, or conspires with any person to engage in such activities." 50 U.S.C. § 1801(b)(1)(B).

For instance, a British national who works for the British embassy in the United States is an agent of a foreign power. American citizens and permanent residents are "agents" if they knowingly engage in espionage for a foreign power or intelligence service, and such activities "are about to involve" a violation of U.S. laws--any criminal laws, not just espionage. §1801(b)(2)(B).

If the target is a "U.S. person," which includes permanent resident aliens and associations and corporations substantially composed of U.S. citizens or permanent resident aliens, 50 U.S.C.A. § 1801 (i), there must be probable cause to believe that the U.S. person's activities "may" or "are about to" involve a violation of the criminal statutes of the United States. § 1801(b)(2)(A),(B); see also § 1801(b)(2)(C) (knowingly engages in activities in preparation for sabotage or "international terrorism" on behalf of a foreign power); § 1801(b)(2)(D) (knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power).

A "United States person" may not be determined to be an agent of a foreign power "solely upon the basis of activities protected by the first amendment to the Constitution of the United States." 50 U.S.C. § 1805(a)(3)(A).

Under 50 U.S.C. §1801(e)(1), "foreign intelligence" information (FII) is information that "relates to" U.S. ability to protect against:

1. possible hostile acts of a foreign power or an agent of a foreign power,
2. sabotage or terrorism by a foreign power or agent, and
3. clandestine intelligence activities by a foreign power or agent.

FII includes information with respect to a foreign power or foreign territory that "relates to" the national defense, national security, or conduct of foreign affairs of the United States. § 1801(e)(2). Under both sections, if the intended surveillance target is a U.S. person, the information must instead be "necessary to" U.S. self-protective ability or U.S. national defense, national security, or foreign affairs. The difference between "relates to" and "necessary to" is undefined in the statute, although there may exist a secret FISA "case law."

Note that because the key FISA definitions are not tied to criminal conduct or even conspiracies, FISA can extend to FII in plain public view or in open archives (such as legal photographs of a city, a facility, or a public street, or newspaper clippings copied from a "morgue").

FISA surveillances must have an intelligence purpose. 50 U.S.C. §1804 (a) (7)(B). But courts allow FISA-obtained information to be used in criminal trials. See, e.g., Exec. Order No. 12,333, 3 C.F.R. 200, 211 (1982), reprinted in 50 U.S.C. § 401 note (1994) (allowing the dissemination of information incidentally obtained during intelligence gathering that indicates activities potentially violating any law).

Courts that have allowed evidence gathered during the surveillance to support a criminal conviction have required that intelligence be the "primary" purpose of the surveillance. *United States v. Humphrey*, 456 F. Supp. 51 (E.D. Va. 1978), aff'd sub nom. *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980), ("the Executive Branch need not always obtain a warrant for foreign intelligence surveillance"), cert. denied, 454 U.S. 1144 (1982); *United States v. Megahey*, 553 F. Supp. 1180, 1189-90 (E.D.N.Y. 1982), aff'd sub nom. *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984).

In the Megahey litigation, the district court found that the phrase "primary purpose" is the guidepost for FISA-derived surveillance, given that "Congress clearly viewed arrest and criminal prosecution as one of the possible outcomes of a foreign intelligence investigation." The Second Circuit agreed, noting that, it is foreseeable that collected intelligence may be used in a criminal proceeding and "Congress recognized that in many cases the concerns of government with respect for foreign intelligence will overlap with those with respect to law enforcement." See also *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991) (holding that the fact that the terrorist activity was directed at Northern Ireland was of no consequence to the legality of the FISA surveillance); *United States v. Pelton*, 835 F.2d 1067, 1076 (4th Cir. 1987) (concluding that "FISA surveillance is not tainted simply because the government can anticipate that the fruits of the surveillance may later be used... in a criminal trial").

FISA powers are broad and vague, and the secrecy of FISA proceedings makes FISA powers susceptible to abuse. FISA power extends well beyond spies and terrorists. It can be used in connection with ordinary criminal investigations involving United States citizens who live in this country and who may be charged with offenses such as narcotics violations or breaches of an employer's confidentiality. 50 U.S.C. §§ 1806, 1825.

For instance, electronic surveillance under § 1801(f)(1) only reaches wire or radio communications "sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person" and a warrant would ordinarily be required. If the U.S. person is not "known," or more important, not "intentionally" targeted, it simply isn't "electronic surveillance" under § 1801(f)(1).

Note also that FISA expressly contemplates that it will produce "unintentionally acquired information."

§ 1806(i). But while this section requires the destruction of such information, it only applies to "the contents of any radio communication," only if a warrant would have been required, and only if both the sender and intended recipients are within the United States.

Given these limits, one may presume that "unintentionally acquired information" outside these lines is not destroyed. That would include all "unintentionally acquired" wire or electronic communications.

Under FISA, requests for counterintelligence warrants are funneled through the Justice Department, which reviews applications by the CIA as well as other agencies before submitting them to the FISA court. 50 U.S.C. §§ 1804(a), 1822(a)(1) (1994). Each application to the FISA court must first be personally approved by the Attorney General. See 50 U.S.C. § 1804(a). The application must contain, among other things, a statement of reasons to believe that the target of the surveillance is a foreign power or agent of a foreign power, specified information on the implementation of the surveillance, and a "certification" from a high-ranking executive branch official stating that the official "deems the information sought to be foreign intelligence information" and that the information sought "cannot reasonably be obtained by normal investigative techniques."

See generally 50 U.S.C. §§ 1804(a)(7), 1805(a) (setting forth the findings necessary to support the issuance of an order authorizing surveillance).

Particular facts or representations required include:

- statements regarding all previous applications involving the target
- "detailed description of the nature of the information sought and of the type of communication or activities to be subject to the surveillance," § 1804(a)(6)
- the length of time surveillance is required, § 1804(a)(10)
- whether physical entry into a premises is necessary, and
- proposed procedures to minimize the acquisition, use, and retention of information concerning nonconsenting U.S. persons. § 1804(b).

On the basis of the application, a FISC judge must find probable cause that the target is a foreign power or agent of a foreign power, and that the facilities where the surveillance is directed are or will be used by the target.

For U.S. persons, the FISC judge must find probable cause that one of four conditions has been met:

1. the target knowingly engages in clandestine intelligence activities on behalf of a foreign power which "may involve" a criminal law violation
2. the target knowingly engages in other secret intelligence activities on behalf of a foreign power pursuant to the direction of an intelligence network and his activities involve or are about to involve criminal violations
3. the target knowingly engages in sabotage or international terrorism or is preparing for such activities or
4. the target knowingly aids or abets another who acts in one of the above ways.

Courts have attached conditions to the executive's use of warrantless surveillance, including the requirement that the President or Attorney General authorize the search, the search targets a foreign power or its agents, and the primary purpose of the search is to gather foreign intelligence information. See Exec. Order No. 12,333, § 2.5, 3 C.F.R. 200 (1982), reprinted in 50 U.S.C. § 401 note (1994)

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

(requiring approval of attorney general for warrantless searches).

An order of the FISC may approve electronic surveillance of an agent of a foreign power for ninety days and of a foreign power for a year. Extensions may be granted on the same terms, except that targets who are foreign powers may be subject to surveillance for an additional year if there is probable cause to believe that no communication of any U.S. person will be acquired.

Suppose a defendant moves to suppress evidence obtained via FISA surveillance. FISA provides that the district court must review in camera and ex parte the FISA application and other materials necessary to rule upon a defendant's suppression motion "if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States." 50 U.S.C. § 1806(f). See United States v. Belfield, 692 F.2d 141, 147 (D.C.Cir.1982) ("The language of section 1806 (f) clearly anticipates that an ex parte, in camera determination is to be the rule. Disclosure and an adversary hearing are the exception, occurring only when necessary.").

In such circumstances, neither defendant nor defendant's counsel is likely to have access to the underlying information. 50 U.S.C. § 1806(f) (The district court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.").

FISA does authorize surveillance without a court order. In general, the Justice Department may engage in electronic surveillance to collect FII without a court order for periods up to one year. 50 U.S.C. § 1802. There must be no "substantial likelihood" that the intercepted communications include those to which a U.S. person is a party. § 1802(a)(1)(B).

Such electronic surveillance must be certified by the Attorney General and then noticed to the Senate and House intelligence committees. § 1802(a)(2). A copy of the certification must be filed with the FISC, where it remains sealed unless (a) an application for a warrant with respect to it is filed, or (b) the legality of the surveillance is challenged in another federal district court under § 1806(f). § 1802(a)(3). Common carriers must assist in the surveillance and maintain its secrecy. § 1802(a)(4).

In emergencies, the Attorney General may authorize immediate surveillance but must "as soon as practicable, but not more than twenty-four hours" later, seek judicial review of the emergency application. § 1805(e).

Constitutionality

Lower courts have found FISA constitutional. See e.g., *United States v. Duggan*, 743 F.2d 59(2d Cir. 1984); *United States v. Belfield*, 692 F.2d 141 (D.C.Cir 1982); *United States v. Nicholson*, 955 F.Supp. 588 (E.D. Va. 1997).

In *United States v. U.S. District Court*, the Supreme Court used a two-part Fourth Amendment reasonableness test. It is doubtful whether the FISA review process satisfies the Court's first measure of the reasonableness of warrantless surveillance -- whether the citizens' interest in privacy and free expression are better served by a warrant requirement. The second element --whether a judicially imposed law enforcement warrant requirement would "unduly frustrate the efforts of Government to

protect itself" -- may be more easily met in the foreign intelligence setting. But Title III has for more than 30 years required more stringent procedures for criminal investigatory wiretaps.

(Taken from FISA FAQ prepared by Lee Tien, Electronic Frontier Foundation Senior Counsel, Sep. 27, 2001. Foreign Intelligence Surveillance Act Used without permission.) (b)(3)-P.L. 86-36

Retrieved from [redacted]
Categories: Intelligence | United States Government | Law

UNCLASSIFIED

- This page has been accessed 11,577 times.
- 7 watching users
- This page was last modified 02:24, 2 July 2014 by [redacted]. Most recent editors: [redacted] and [redacted] (b)(6)

linipedweb6s

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

[redacted]

(U) Foreign Intelligence Surveillance Act

UNCLASSIFIED

From Intellipedia

You have new messages (last change).

This acronym-related article is a stub. You can help Intellipedia by expanding it.

This article is a collaboration request.

All Intellipedians are invited to collaborate and contribute information that may help further develop this article. Please use section editing (i.e. only edit the section you want to work on) and save often to minimize edit conflicts. To discuss issues or air disputes regarding information on this article, please use the discussion page.

- Anyone have the act that can be placed/linked in here? [redacted] 19:38, 19 December 2008 (UTC) (b) (6)

PUBLIC LAW 95–511 October 25, 1978 Foreign Intelligence Surveillance Act of 1978 [1]

PUBLIC LAW 110–261 July 10, 2008 Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 [2] (b) (3)-P.L. 86-36

Retrieved from [redacted]
Categories: Acronym stubs | Collaboration Requests

UNCLASSIFIED

- This page has been accessed 1,193 times.
- 1 watching user
- This page was last modified 21:04, 6 March 2009 by [redacted] Most recent editors: [redacted] (b) (6)

[redacted] (b) (3)-P.L. 86-36

(U) Foreign Intelligence Surveillance Act of 1978

UNCLASSIFIED//~~FOUO~~

From Intellipedia

(Redirected from Foreign Intelligence Surveillance Act)
You have new messages (last change).

The **Foreign Intelligence Surveillance Act (FISA)** of 1978 prescribes procedures for the physical and electronic surveillance and collection of "foreign intelligence information" between or among "foreign powers" on territory under United States control.

FISA is codified in 50 U.S.C. §§1801-1811, 1821-29, 1841-46, and 1861-62.[1] The subchapters of FISA provide for:

- Electronic Surveillance
- Physical Searches
- Pen Registers and Trap & Trace Devices for Foreign Intelligence Purposes
- Access to certain Business Records for Foreign Intelligence Purposes

The Act was amended by the FISA Amendments Act of 2008 (FAA) (H.R. 6304), which established a procedure for authorizing certain acquisitions of foreign intelligence, among other purposes. It had been earlier amended by the USA PATRIOT Act of 2001, primarily to include terrorism on behalf of groups that are not specifically backed by a foreign government, and the Protect America Act of 2007, signed into law on 5 August 2007, provisions of which were extended by FAA.

Contents

- 1 Dissemination Rules for FISA Information
- 2 FISA information on Intellipedia
- 3 History
- 4 Scope and limits
- 5 Provisions
  - 5.1 Electronic surveillance
    - 5.1.1 Without a court order
    - 5.1.2 With a court order
  - 5.2 Physical Searches
  - 5.3 FISA court
  - 5.4 Remedies for violations
  - 5.5 Lone wolf amendment
- 6 Constitutionality
  - 6.1 Before FISA

- 6.2 Post FISA
- 6.3 Foreign intelligence warrant exception
- 7 Criticisms
- 8 Proposed amendments
- 9 See also
- 10 References

Dissemination Rules for FISA Information

(U//~~FOUO~~) The "FISA" portion mark does NOT limit the distribution of reports and/or tear lines. There is no special clearance or access required to read disseminated FISA/FAA information. It is important to differentiate between access to raw FISA/FAA collection and access to disseminated FISA/FAA information. Special training and accesses are required to gain access to raw FISA/FAA collection, but NOT to be able to read disseminated FISA/FAA information.

FISA information on Intellipedia

FISA

(U) This section/page contains information that is **FISA** derived.

(U) Do not use **FISA** information in a criminal proceeding or disseminate to a foreign government without Attorney General authorization.

FISA information is allowed as long as it is within the overall classification limits of JWICS (TS//SI/TK/NF) and that it is appropriately marked. Please add the {{FISA}} banner template to any page that includes FISA derived material. **Contact your Security Officer for an official answer from the perspective of your organization's data.** See Talk:Foreign Intelligence Surveillance Act of 1978#FISA on Intelink for discussion about this topic. Should you have citable references to formal policy/guidance on posting of FISA to Intelink, please provide that information on the talk page.

For additional information about what information is allowed on Intelink, see Intellipedia:Classification Policy

History

The Foreign Intelligence Surveillance Act resulted from extensive investigations into domestic intelligence activities by Senate Committees, led separately by Sam Ervin and Frank Church in the 1970s (see the Church Committee report).

Founding Date: 1974

Founding Directive or Legislation: Foreign Intelligence Act of 1974 (FISA)

Charter Summary or Description: The FISC implements the Foreign Intelligence Act, which authorizes

electronic surveillance and physical searches, without consent, on groups and individuals inside the United States for the purpose of collecting "foreign intelligence."

Membership: The court is composed of eleven U.S. District court judges who are appointed to the FISA Court by the Chief Justice of the Supreme Court to serve for seven years. The Court of Review consists of three U.S. District Court of Appeals judges.

Source: Central Intelligence Agency, A Consumer's Guide to Intelligence (Langley, Va.: Office of Public Affairs, CIA, 2000), p. 44.

The Act came into public prominence in December 2005 following publication by the *New York Times* of an article[2] that described a program of warrantless domestic wiretapping ordered by the Bush administration and carried out by the National Security Agency since 2002 (a subsequent Bloomberg article[3] suggested that this may have already begun by June 2000). Many critics have asserted that the Administration's warrantless spying program is a criminal violation of FISA. The Bush administration, while conceding that it does not follow FISA, asserts that the program is nonetheless legal on the grounds that FISA is an unconstitutional infringement of executive power and/or FISA was implicitly amended or abrogated by the Authorization for Use of Military Force resolution passed by Congress.

The Attorney General Gonzales in a speech at Georgetown University on 24 January 2006 said: [4]

> Just a few days after the events of September 11th, Congress enacted a joint resolution to support and authorize a military response to the attacks on American soil. In this resolution, the Authorization for Use of Military Force, Congress did two important things. First, it expressly recognized the President's "authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." Second, it supplemented that authority by authorizing the President to, quote, "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" in order to prevent further attacks on the United States.

Scope and limits

For most purposes, including electronic surveillance and physical searches, "foreign powers" means a foreign government, any faction(s) of foreign governments not substantially composed of US persons, and any entity directed or controlled by a foreign government. §§1801(a)(1)-(3) The definition also includes groups engaged in international terrorism and foreign political organizations. §§1801(a)(4) and (5). The sections of FISA authorizing electronic surveillance and physical searches without a court order specifically exclude their application to groups engaged in international terrorism. *See* §1802(a)(1) (referring specifically to §1801(a)(1), (2) and (3)).

The statute limits its application to US persons. A US person includes citizens, lawfully admitted permanent resident aliens, and corporations incorporated in the US.

The code defines "foreign intelligence information" to mean information necessary to protect the United States against actual or potential grave attack, sabotage or international terrorism.[5]

Provisions

Electronic surveillance

Generally, the statute permits electronic surveillance in two scenarios.

Without a court order

The President may authorize, through the Attorney General, electronic surveillance without a court order for the period of one year provided it is only for foreign intelligence information [5]; targeting foreign powers as defined by 50 U.S.C. §1801(a)(1),(2),(3) [6] or their agents; and there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party.[7]

The Attorney General is required to make a certification of these conditions under seal to the Foreign Intelligence Surveillance Court[8], and report on their compliance to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. [9]

Since 50 U.S.C § 1802 (a)(1)(A) of this act specifically limits warrantless surveillance to foreign powers as defined by 50 U.S.C. §1801(a) (1),(2), (3) and omits the definitions contained in 50 U.S.C. §1801(a) (4),(5),(6) the act does not authorize the use of warrantless surveillance on: groups engaged in international terrorism or activities in preparation therefore; foreign-based political organizations, not substantially composed of United States persons; or entities that are directed and controlled by a foreign government or governments. [10] Under the FISA act, anyone who engages in electronic surveillance except as authorized by statute is subject to both criminal penalties [11] and civil liabilities. [12]

With a court order

Alternatively, the government may seek a court order permitting the surveillance using the FISA court.[13] Approval of a FISA application requires the court find probable cause that the target of the surveillance be a "foreign power" or an "agent of a foreign power", and that the places at which surveillance is requested are used or will be used by that foreign power or its agent. In addition, the court must find that the proposed surveillance meet certain "minimization requirements" for information pertaining to US persons[14].

Physical Searches

In addition to electronic surveillance, FISA permits the "physical search" of the "premises, information, material, or property used exclusively by" a foreign power.

The requirements and procedures are nearly identical to those for electronic surveillance.

FISA court

Main article: United States Foreign Intelligence Surveillance Court

The Act created the Foreign Intelligence Surveillance Court (FISC) and enabled it to oversee requests for surveillance warrants by federal police agencies (primarily the F.B.I.) against suspected foreign intelligence

agents inside the U.S. The court is located within the Department of Justice headquarters building. The court is staffed by eleven judges appointed by the Chief Justice of the United States to serve seven year terms.

Proceedings before the FISA court are *ex parte* and non-adversarial. The court hears evidence presented solely by the Department of Justice. There is no provision for a release of information regarding such hearings, or for the record of information actually collected.

Main article: United States Foreign Intelligence Surveillance Court of Review

Denials of FISA applications by the FISC may be appealed to the Foreign Intelligence Surveillance Court of Review. The Court of Review is a three judge panel which has published opinions in only two cases. In the first, in 2002, the federal government contested restrictions the FISA court imposed that would have limited the Justice Department's ability to use information gained through FISA to "enhance criminal prosecution." The second, in 2008, was brought against a service provider who resisted a FISA court order to assist the government in collecting information about a customer. The government won both cases.

Remedies for violations

Both the subchapters covering physical searches and electronic surveillance provide for criminal and civil liability for violations of FISA.

Criminal sanctions follows violations of electronic surveillance by *intentionally* engaging in electronic surveillance under the color of law or through disclosing information known to have been obtained through unauthorized surveillance. The penalties for either act are fines up to $10,000, up to five years in jail, or both.[11]

In addition, the statute creates a cause of action for private individuals whose communications were unlawfully monitored. The statute permits actual damages of not less than $1,000 or $100 per day. In addition, that statute authorizes punitive damages and an award of attorney's fees.[12]

Similar liability is found under the subchapter pertaining to physical searches.

In both cases, the statute creates an affirmative defense for a law enforcement agent acting within their official duties and pursuant to a valid court order. Presumably, such a defense is not available to those operating exclusively under presidential authorization.

Lone wolf amendment

In 2004, FISA was amended to include a "lone wolf" provision. 50 U.S.C. §1801(b)(1)(C). A "lone wolf" is a non-US person who engages in or prepares for international terrorism. The provision amended the definition of "foreign power" to permit the FISA courts to issue surveillance and physical search orders without having to find a connection between the "lone wolf" and a foreign government or terrorist group.[15]

Constitutionality

Before FISA

In 1967, the Supreme Court of the United States held that the requirements of the Fourth Amendment applied equally to electronic surveillance and to physical searches. *Katz v. United States*, 389 U.S. 347 (1967). The

Court did not address whether such requirements apply to issues of national security. Shortly after, in 1972, the Court took up the issue again in *United States v. United States District Court, Plamondon,* where the court held that court approval was required in order for the domestic surveillance to satisfy the Fourth Amendment. 407 U.S. 297 (1972). Justice Powell wrote that the decision did not address the requirements of the Fourth Amendment "may be involved with respect to activities of foreign powers or their agents."

In the time immediately preceding FISA, a number of courts squarely addressed the issue of "warrantless wiretaps". In both *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973), and *United States v. Butenko*, 494 F.2d 593 (3rd Cir. 1974), the courts upheld warrantless wiretaps. In *Brown*, a US citizen's conversation was captured by a wiretap authorized by the Attorney General for foreign intelligence purposes. In *Butenko*, the court held a wiretap valid if the primary purpose was for gathering foreign intelligence information.

A plurality opinion in *Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975), held that a warrant was required for the domestic surveillance of a domestic organization. In this case, the court found that the domestic organization was not a "foreign power or their agent", and "absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional."

Post FISA

There have been very few cases involving the constitutionality of FISA. In two lower court decisions, the courts found FISA constitutional. In the *United States v. Duggan*, the defendants were members of the Irish Republican Army. 743 F.2d 59 (2nd Cir., 1984). They were convicted for various violations regarding the shipment of explosives and firearms. The court held that their compelling considerations of national security in the distinction between the treatment of U.S. citizens and non-resident aliens.

In the *United States v. Nicholson*, the defendant moved to suppress all evidence gathered under a FISA order. 955 F.Supp. 588 (Va. 1997). The court affirmed the denial of the motion. There the court flatly rejected claims that FISA violated Due process clause of the Fifth Amendment, Equal protection, Separation of powers, nor the Right to counsel provided by the Sixth Amendment.

However, in a third case, the special review court for FISA, the equivalent of a Circuit Court Of Appeals, opined differently should FISA limit the President's inherent authority for warrantless searches in the foreign intelligence area. In *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002) the special court stated "[A]ll the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information . . . . We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power."

Foreign intelligence warrant exception

FISA regulates the surveillance and collection for foreign intelligence domestically. Notably, FISA does not control extra-territorial intelligence operations. Courts, including the District Court for the Southern District of New York, have adopted a "foreign intelligence exception" to ordinary requirements for warrants.[16]

Criticisms

K. A. Taipale of the World Policy Institute, James Jay Carafano of the Heritage Foundation[17], and Philip Bobbitt of the University of Texas Law School,[18] among others,[19] have argued that FISA may need to be amended (to include, among other things, procedures for programmatic approvals) as it may no longer be

adequate to address certain foreign intelligence needs and technology developments, including: the transition from circuit-based communications to packet-based communications; the globalization of communications infrastructure; and the development of automated monitoring techniques, including data mining and traffic analysis.[20]

The need for programmatic approval of technology-enabled surveillance programs is particularly crucial in foreign intelligence. See, for example, John R. Schmidt, the associate attorney general (1994-1997) in the Justice Department under President Bill Clinton,[21] recalling early arguments made by then-Attorney General Edward Levi to the Church Committee that foreign intelligence surveillance legislation should include provisions for programmatically authorizing surveillance programs because of the particular needs of foreign intelligence where "virtually continuous surveillance, which by its nature does not have specifically predetermined targets" may be required. In these situations, "the efficiency of a warrant requirement would be minimal."

And, in a recent essay, Judge Richard A. Posner opined that FISA "retains value as a framework for monitoring the communications of known terrorists, but it is hopeless as a framework for detecting terrorists. [FISA] requires that surveillance be conducted pursuant to warrants based on probable cause to believe that the target of surveillance is a terrorist, when the desperate need is to find out who is a terrorist."[22]

Proposed amendments

On March 16, 2006, Senators Mike DeWine (R-OH), Lindsey Graham (R-SC), Chuck Hagel (R-NE), and Olympia Snowe (R-ME) introduced the Terrorist Surveillance Act of 2006 (S.2455),[23][24] under which the President would be given certain additional limited statutory authority to conduct electronic surveillance of suspected terrorists in the United States subject to enhanced Congressional oversight. Also on March 16, 2006, Senator Arlen Specter (R-PA) introduced The National Security Surveillance Act of 2006 (S.2453),[25][26] which would amend FISA to grant retroactive amnesty[27] for warrantless surveillance conducted under presidential authority and provide FISA court (FISC) jurisdiction to review, authorize, and oversight "electronic surveillance programs." On May 24, 2006, Senator Specter and Senator Dianne Feinstein (D-CA) introduced the Foreign Intelligence Surveillance Improvement and Enhancement Act of 2006 (S.3001) asserting FISA as the exclusive means to conduct foreign intelligence surveillance.

All three of these competing bills have been the subject of Judiciary Committee hearings throughout the summer.[28] On September 13, 2006, the Senate Judiciary Committee voted to approve all three mutually exclusive bills, thus, leaving it to the full Senate to resolve.[29]

On July 18, 2006, U.S. Representative Heather Wilson (R-NM) introduced the Electronic Surveillance Modernization Act (H.R. 5825). Wilson's bill would give the President the authority to authorize electronic surveillance of international phone calls and e-mail linked specifically to identified terrorist groups immediately following or in anticipation of an armed or terrorist attack on the United States. Surveillance beyond the initial authorized period would require a FISA warrant or a presidential certification to Congress. On September 28, 2006 the House of Representatives passed Wilson's bill and it was referred to the Senate.[30]

See also

- Watergate
- Church Committee

Intelligence History Portal

[redacted]

DOCID: 4321869

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

- USA PATRIOT Act
- Text of FISA on Intelink [redacted]
- Intelligence Community Oversight Discussion

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

References

1. ↑ 50 U.S.C Chapter 36 Foreign Intelligence Surveillance (http://www.law.cornell.edu/usco de /html/uscode50/usc_sup_01_50_10_ 36.html) The complete text of the Foreign Intelligence Surveillance Act
2. ↑ "Bush Lets US Spy on Callers Without Courts" (16 December2005; [1] (http://www.commondreams .org/headlines05/1216-01.htm)
3. ↑ http://www.bloomberg.com/apps/n ews?pid=20601087&sid=abIV0cO64zJE& refer=
4. ↑ http://www.fas.org/irp/news/200 6/01/ag012406.html
5. ↑ [5.0] [5.1] 50 U.S.C. §1801(e) (http://www.law.cornell.edu/uscode/html/uscode50 /usc_sec_50_00001801----000-.htm l#e) Definition of Foreign intelligence information
6. ↑ 50 U.S.C. §1801(a) (http://www.law.cornell.edu/uscode/html/uscode50 /usc_sec_50_00001801----000-.htm l#a) Definition of Foreign power
7. ↑ 50 U.S.C. sect;1802(a)(1) (http://www.law.cornell.edu/uscode/html/usco de50 /usc_sec_50_00001802----000-.htm l#a_1) Conditions under which the President, through the Attorney General, may authorize electronic surveillance without a court order
8. ↑ 50 U.S.C. sect;1802(a)(3) (http://www.law.cornell.edu/uscode/html/usco de50 /usc_sec_50_00001802----000-.htm l#a_3) Requirement of the Attorney General's to file reports under seal on warrantless surveillance to the FISC
9. ↑ 50 U.S.C. sect;1802(a)(2) (http://www.law.cornell.edu/uscode/html/usco de50 /usc_sec_50_00001802----000-.htm l#a_2) Requirement of the Attorney General's to report on compliance with warrantless surveillance requirements to Congress
10. ↑ 50 U.S.C. sect;1802 (a)(1)(A) (http:// www.law.cornell.edu/uscode/html/ uscode50 /usc_sec_50_00001802----000-.htm l#a_1_A) The limitation of warrantless surveillance to foreign powers as defined in 50 U.S.C § 1801 (a) (1),(2), and (3)
11. ↑ [11.0] [11.1] 50 U.S.C. §1809 (http://www.law.cornell.edu/usco de/html/uscode50 /usc_sec_50_00001809----000-.htm l) - Criminal sanctions
12. ↑ [12.0] [12.1] 50 U.S.C. §1810 (http://www.law.cornell.edu/usco de/html/uscode50 /usc_sec_50_00001810----000-.htm l) - Civil liability
13. ↑ 50 U.S.C §1805 (http://www.law.cor nell.edu/uscode/html/uscode50 /usc_sec_50_00001805----000-.htm l) Electronic surveillance with a court order
14. ↑ 50 U.S.C. §1801(5) (http://www.law.cornell.edu/uscode/html/uscode50 /usc_sec_50_00001801----000-.htm l#h) Minimization procedures definition
15. ↑ "Lone Wolf" Amendment to the Foreign Intelligence Surveillance Act
16. ↑ *United States v. Bin Laden* , 126 F.Supp.2d 264 (S.D.N.Y. 2000)
17. ↑ Commentary (http://www.washingtontimes.com/commenta ry/20060124-104527-1255r.htm) , Wash. Times, Jan. 24, 2006
18. ↑ Why We Listen (http://www.nytim es.com/2006/01/30/opinion/30bobb itt.html?ex=1139374800& en=c455580a2c60431a&ei=5070) , N.Y. Times, Jan. 30, 2006
19. ↑ The Eavesdropping Debate We Should be Having (http://www.denverpost.com/searc h/ci_3469783)
20. ↑ *Whispering Wires and Warrantless Wiretaps (http://ssrn.com/abstract=889120)*
21. ↑ "A historical solution to the Bush spying issue (http://www.chica gotribune.com/news/opinion

[redacted]

DOCID: 4321869

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

/chi-0602120419feb12,0,6895976.s tory?coll=chi-newsopinioncomme ntary-hed) ," Chicago Tribune (Feb. 12, 2006)

22. ↑ A New Surveillance Act (http://online.ws j.com/article/SB1139967435900741 83-search.html) , Wall Street Journal February 15, 2006
23. ↑ Press Release of Senator DeWine (http ://www.fas.org/irp/congr ess/2006_cr/dewine031606.html)
24. ↑ Dewine Bill as introduced
25. ↑ Specter Floor Statement
26. ↑ Specter Bill as introduced
27. ↑ Specter Offers Compromise on NSA Surveillan ce (http://www.washingt onpost.com/wp-dyn/content /article/2006/06/08/AR2006060801 992.html) , Washington Post, Junc 9, 2006
28. ↑ FIS linking to 2006 FISA Congressional Hearings material (http://www.fas.org/irp/congress /2006_hr /index.html#fisa4)
29. ↑ Conflicting Bills on Warrantless Surveillance Advance in Senate (http://www.fas.org/blog/secrecy /2006/09/conflicting_bills_on_w arrantle.html) , Secrecy News, September 14, 2006
30. ↑ House Passes Wilson FISA Bill (http:// wilson.house.gov/NewsAction.a sp?FormMode=Releases& ID=1309) , Press Release, September 29, 2006.

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

Retrieved from [redacted]

Categories: Classification | Intelligence Collection | Law of the United States | History of Intelligence

UNCLASSIFIED/~~FOUO~~

- This page has been accessed 27,751 times.
- 15 [redacted] watching users

(b)(6)

- This page was last modified 15:35, 11 February 2016 by [redacted]

c2linipedweb5j