

Electronic Frontier Foundation backgrounder and analysis of FISA issues raised by anti-terrorism legislation

This document is divided into two parts. The first part provides background on the the Foreign Intelligence Surveillance Act, which is not well known to most people. The second part provides commentary on how ATA would change FISA.

EFF's general comment here is that FISA is already a danger to civil liberties because judicial oversight of FISA surveillance is markedly less meaningful than practice under Title III. Moreover, the secrecy that surrounds FISA judicial review, whether by the FISA Court or in other courts, reduces the public accountability. To the extent that FISA's terms are broad, vague, or ambiguous, very few people have access to the "case law" that might shed light on FISA's meaning. It is difficult for the rule of law to function in this way.

EFF is skeptical that any expansion of FISA surveillance is warranted. Congress should demand honest, good-faith explanations for any expansion of FISA power, given the Executive Branch's track record of warrantless surveillance.

Contact: Lee Tien, Senior Staff Attorney, tien@eff.org, (415) 436-9333 x 102

FISA backgrounder

1. What is FISA?

FISA is the Foreign Intelligence Surveillance Act, which 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).

2. What is the purpose of FISA?

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. See 50 U.S.C. § 401(a)(3) (defining "counterintelligence" 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.

3. How does FISA fit with regulation of electronic surveillance?

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 (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.

4. Why is there a special legal regime for “foreign intelligence” surveillance?

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 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.

5. Can FISA be used for ordinary criminal investigation?

Yes, but with qualifications. 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 change under ATA.

6. Is there really a secret FISA court?

Yes. 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, along with an inventory of items taken, or 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.

7. What kind of surveillance can be authorized under FISA?

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.

8. How is surveillance authority different under FISA?

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 -- and it isn't. 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.

9. What is the basic "trigger" for permitting FISA surveillance?

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).

10. What is a "foreign power"?

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 do "foreign-based," "political," "organization," and "substantially" mean? Would FISA include a group of foreign college or graduate students that engages in political activism? A group of people who exchange opinions about world affairs by e-mail, some of whom live in the United States and others abroad?

11. What is an “agent of a foreign power”?

§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).

So, 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).

12. So FISA doesn't treat aliens and U.S. citizens equally?

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).

13. What is “foreign intelligence” information (FII)?

Under 50 U.S.C. §1801(e)(1), 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").

14. Can the FBI use FISA surveillance to get evidence for criminal prosecution?

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").

15. Why is FISA dangerous?

Most important, 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.

16. How does FISA work?

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) (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.

17. What happens if a criminal defendant challenges the validity of FISA surveillance?

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.").

18. Does FISA authorize surveillance without a court order?

Yes. First, the President, through the Attorney General, may authorize electronic surveillance to collect FII without a court order for periods up to one year. 50 U.S.C. § 1802. This authority can only be used on a written certification that such surveillance is either "solely directed" at communications between or among foreign powers, or focused on a technical intelligence from property or premises "under the open and exclusive control of a foreign power." 50 U.S.C. § 1802(a)(1)(A)(i), (ii). Also, 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).

Second, 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).

How ATA changes FISA

ATA is defended on the basis of needing to meet the threat of terrorism. But ATA's expansion of FISA powers is not limited to terrorism cases. It must not be forgotten that a major reason for FISA was a well-documented record of executive branch abuse of national security surveillance powers.

Second, the government essentially claims that FISA is more restrictive than other surveillance statutes, and that FISA should "more closely track" such other laws. This argument strikes EFF as disingenuous, because the government's special FISA powers are sui generis, intended only for gathering intelligence about foreign powers for counterintelligence purposes.

Third, a recurring theme of ATA is the elimination of the requirement that FISA surveillance be limited to "agents of a foreign power." This requirement protects U.S. persons (citizens and permanent resident aliens), to some extent, against FISA surveillance. Removing this requirement is likely to increase FISA surveillance of U.S. persons. Non-U.S. persons, of course, are also entitled to Fourth Amendment protection.

Sec. 104. Savings provision.

Present 18 USC Sec. 2511(2)(f) says that the procedures of Title III and FISA are "the exclusive means by which electronic surveillance, as defined in [FISA, 50 USC Sec. 1801], and the interception of domestic wire, oral, or electronic communications may be conducted."

However, present 18 USC Sec. 2511(2)(f) does not mention Ch. 206 of Title 18, 18 USC §§ 3121 et seq., which regulates the use of pen register and trap-and-trace devices. ATA 104 provides that the pen/trap statute does not affect the gathering of foreign intelligence information from international or foreign communications. It also provides that the pen/trap statute does not affect FISA electronic surveillance under 50 USC § 1801(f)(4), which regulates the acquisition of "information" (as opposed to "contents") from oral and electronic communications by device "in the United States" when there is a reasonable expectation of privacy and a warrant would be required under Title III. Therefore, the effect of ATA 104 is to make certain that the pen/trap statute has no effect on the use of pen/trap devices under FISA. Essentially, all FISA pen/trap use would be governed by FISA's own pen/trap provisions. See discussion below of ATA 155.

Sec. 151. Period of orders of electronic surveillance of non-United States persons under foreign intelligence surveillance.

Under current law, FISA authorizes

--electronic surveillance of “agents of a foreign power” for up to 90 days, and of “foreign powers” for up to 1 year. 50 U.S.C. § 1805(e)(1);

--physical searches of “agents of a foreign power” for up to 45 days, and of “foreign powers” for up to 1 year. 50 U.S.C. § 1824(d)(1).

This section would extend the duration of a FISA order to up to one year for “agents of a foreign power” under § 1801(b)(1)(A), which applies to non-U.S. persons, i.e., aliens in the United States who are not permanent residents.

This is a bad idea, because aliens in the United States are entitled to the protection of the Fourth Amendment. Moreover, this extension would apply to surveillance of their home phones and computers, because their offices can already be bugged or wiretapped for a year.

By comparison, Title III provides that ordinary wiretaps may not last more than 30 days, and each successive extension is equally limited. 18 U.S.C. § 2518(4)

Also, it should be remembered that the initial order is based only a showing of probable cause. The point of the 45- and 90-day limits is to require the government to come back and demonstrate, armed with the experience of the initial search or surveillance, that the target truly is an “agent of a foreign power.” Extending the duration of initial order means that persons who are not “agents of a foreign power” are subjected to unjustified search and surveillance for a much longer period.

Sec. 152. Multi-point authority.

FISA does not currently authorize so-called “roving wiretaps.” Roving wiretaps are unlike conventional wiretaps in that they allow law enforcement officials to follow the suspect from one location to the next, without having to seek court authorization to wiretap each location's telephone line or other communication channel. In short, the government may wiretap any telephone that the target uses or is known to use.

Roving wiretaps pose serious problems under the Fourth Amendment, which requires that any search warrant “particularly describ[e] the place to be searched, and the person and things to be seized.” The particularity requirement carefully tailors the scope of search to its justification. *Maryland v. Garrison*, 480 U.S. 79, 84 & n. 8 (1987). An insufficiently particular warrant may constitute an unconstitutional “general warrant” like those used by the British against American colonists -- a prime concern of the Framers. See *Marcus v. Search Warrant*, 367 U.S. 717 (1961); *Stanford v. Texas*, 379 U.S. 476 (1965); *Andresen v. Maryland*, 427 U.S. 453 (1976); and *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 391 (1979).

In *Andresen*, for instance, a real estate attorney was suspected of fraud, and a search warrant was executed on his office. The officers seized substantial information beyond what the warrant specified because of a “catch-all” phrase in the warrant. The Supreme Court held that the “catch-all” phrase made the search general. *Andresen*, 427 U.S. at 479-82.

Equally important, when the Court definitively ruled on the constitutionality of eavesdropping, it made clear that unless the particularity requirement was observed, an officer would have a “roving commission to ‘seize’ any and all conversations.” *Berger*, 388 U.S. at 59. Merely naming the person, the Court said, does not “particularly describ[e] the communications, conversations, or discussions to be seized.” *Ibid*.

This section would expand FISA to include “roving wiretap” authority. Current law requires court-“specified” third parties (like common carriers and ISPs) to provide assistance necessary to accomplish the surveillance. The proposed change would extend that obligation to unnamed and unspecified third parties. According to the Justice Department, “the FBI could simply present the newly discovered carrier, landlord, custodian, or other person with a generic order issued by the Court, and could then effect FISA coverage as soon as technically feasible.”

In practical terms, roving wiretaps pose a greater danger to personal privacy than ordinary wiretaps for two reasons. First, the issuing court in effect gives the government a blank check to do surveillance, because it does not approve particular wiretaps. There simply will not be a showing of probable cause for each wiretap.

Second, by extending surveillance to many more communication channels, the number of potentially innocent conversations of innocent persons increases. “[O]nce a roving intercept order is issued, there is no express limitation on the number of places in which the government can install listening devices or telephones it can tap, and the decision in each instance [is] an executive rather than a judicial one.” 1 Clifford S. Fishman & Anne T. McKenna, *Wiretapping and Eavesdropping* 9-14 (2d ed.1995).

In addition, the particularity problem is especially acute for wiretaps in general, because they involve seizures of speech. As a general rule, if a warrant authorizes the seizure of items for the ideas that they express, it must describe them with “scrupulous exactitude,” such that the officers executing the warrant have no discretion in determining the items to be seized. *Stanford v. Texas*, 379 U.S. 476, 485-86 (1965).

The impact of this amendment would be especially great for communication facilities used by the general public, from public payphones to computers in public libraries. Upon the suspicion that a FISA target might use such a facility, the FBI could monitor all communications transmitted at the facility, and the recipient of the assistance order could not disclose that monitoring is occurring.

Sec. 153. Foreign intelligence information.

Under current law, FISA surveillance may only be used when foreign-intelligence information gathering is “the” sole or “primary” purpose. See FISA Backgrounder, QA15 (citing cases).

This section would permit FISA surveillance even when the main purpose is to investigate a crime, which destroys the existing balance between counterintelligence and law enforcement surveillance.

When the FISA court reviews an application for FISA surveillance, its job is merely to assure that all the necessary certifications -- including the representation that the primary purpose is to gather foreign intelligence information -- are present and not clearly erroneous. Thus, when FISA surveillance is challenged in a criminal proceeding, courts have said that it is “not the function of” the courts “to ‘second-guess’ the certifications.” *United States v. Rahman*, 861 F.Supp. 247, 250 (S.D.N.Y. 1994), affirmed 189 F.3d 88 (2d Cir. 1999), cert. denied 120 S.Ct. 439, 120 S.Ct. 830, 120 S.Ct. 830, 120 S.Ct. 831 (citing *United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984)..

Given that FISA contains far fewer procedural protections than Title III, and that FISA orders are issued and implemented in great secrecy, this is an enormous change in the law.

Sec. 154. Foreign intelligence information sharing.

Under current law, information obtained from non-FISA criminal investigations like federal grand jury investigations may only be disclosed under stringent procedural safeguards.

This section would allow “foreign intelligence information” gathered in such investigations to be shared with federal law enforcement, the intelligence and defense community, and immigration authorities.

The secrecy of grand jury investigations under current law is partly due to the sweeping powers of grand juries to compel the disclosure of information via subpoenas without judicial oversight. The Supreme Court has emphasized that the grand jury “is a grand inquest, a body with powers of investigation and inquisition, the scope of whose inquiries are not to be limited narrowly by questions of propriety or forecasts of the probable result of the investigation, or by doubts whether any particular individual will be found properly subject to an accusation of crime.” *Blair v. United States*, 250 U.S. 273, 283 (1919).

The grand jury can call anyone to testify before it based on a prosecutor’s speculation about possible criminality, and they can be asked to bring documents and other tangible things. Any aspect of a person’s life that might shed some light on criminality by someone is within the scope of a grand jury investigation.

In contrast, the government cannot get an ordinary search warrant to obtain evidence unless it has probable cause.

Thus, this section also upsets the balance between counterintelligence and law enforcement surveillance: it creates an incentive to use grand jury and other investigations as a tool for foreign intelligence collection.

Sec. 155. Pen register and trap and trace authority.

Under current law, pen/trap devices may not be used under FISA unless the government shows that it will be placed on a communications device that has been or will be used in communications with “an agent of a foreign power.” § 1842(c)(3).

This section eliminates that requirement, allowing FISA pen/trap orders to be used on a government certification that it is likely to obtain information relevant to an ongoing foreign intelligence or international terrorism investigation.

Thus, FISA pen/trap surveillance could be used against any person, not only agents of foreign powers. This eliminates two key protections for U.S. persons under FISA (as opposed to non-resident aliens). First, there would be no showing that the U.S. person was involved in some kind of criminality, which is needed for a U.S. person to be an agent of a foreign power. § 1801(b)(2). Second, it would evade the FISA constraint that a U.S. person cannot be deemed an “agent of a foreign power” solely on the basis of First Amendment activities. § 1805(a)(3)(A).

Sec. 156. Business records.

Under current law, a limited set of records -- those of common carriers, public accommodation facilities, physical storage facilities, and vehicle rental facilities -- can be obtained with a court order. 50 U.S.C. § 1861-62.

This section gives the government the authority to obtain “any tangible things,” including documents, via administrative subpoena, so long as they are relevant to a foreign intelligence or international terrorism investigation.

This section greatly expands the scope of the “business records” provision. Moreover, the use of subpoena power eliminates the possibility of judicial oversight, because a court order would be unnecessary.

The government’s only argument for this substantial change is that “[t]he time and difficulty involved in getting such pleadings before the Court usually outweighs the importance of the business records sought.” This strikes EFF as remarkably weak. If the records are not important, then the authority is unnecessary. If the records are, in fact, important, then it should be worth applying for a court order. Note also that the government’s section-by-section analysis does not even mention that ATA would expand the scope of this section to business records in general.

Sec. 157. Miscellaneous national-security authorities.

Current law generally requires that government access under FISA to a variety of records (governed by the Fair Credit Reporting Act, the Financial Right to Privacy Act, ECPA) is conditioned on a showing by “specific and articulable facts” that there is reason to believe that the entity, person or consumer is an “agent of a foreign power.”

This section would eliminate this requirement and permit such access if the government certifies that the information is “relevant to an authorized foreign counterintelligence investigation.”

Not only does this lessen the government’s factual burden, it removes the protections for U.S. persons that accompany the “agent of a foreign power” requirement.

Sec. 158. Disclosure of educational records.

The Federal Education Rights and Privacy Act protects the privacy of various educational records. This section would permit government access to such records if “any” federal employee designated by the Attorney General or Secretary of Education determines that the records can reasonably be expected to assist in investigating or preventing terrorism.

Note that because ATA Sec. 309 defines many computer crimes unrelated to terrorism as “Federal terrorism offenses,” this section would eliminate student privacy for all records that might relate to investigating such crimes. This represents a significant violation of privacy unrelated to the ATA’s purported anti-terrorism justification.

USAA

Sec. 207: authorizes FISA roving wiretaps

**Sec. 208: extends duration of FISA surveillance, but better than ATA
doesn’t extend for physical searches**