

Foreign Intelligence Surveillance

The Foreign Intelligence Surveillance Act, 50 U.S.C. sec. 1801 *et seq.* (FISA), was passed in 1978. It was a response to previous actions by the Executive branch of the United States government. FISA's purpose was to strike a balance between the government's legitimate interest in protecting national security, and the rights of U.S. citizens under the Fourth Amendment. Every president since Franklin D. Roosevelt has asserted and utilized the authority to authorize warrantless electronic surveillance to collect foreign intelligence in the interests of national security. This power was granted a great amount of judicial and congressional deference until the early 1970's, and extended to the executive's gathering of both domestic and foreign intelligence.

The National Security Act, Public Law 80-253, enacted in July 26, 1947, established a statutory framework for the managerial structure of the United States intelligence community, including the Central Intelligence Agency (CIA) and the position of Director of Central Intelligence (DCI). The act also created a semi-unified military command structure under a Secretary of Defense, and a National Security Council (NSC) to advise the President “with respect to the integration of domestic, foreign, and military policies relating to the national security.”

At the creation of the Central Intelligence Agency in 1947, the President and the Congress collaborated in issues involving surveillance related to national security. Recognizing the essential purpose of intelligence gathering, initial modifications of the CIA and related intelligence agencies were focused on efficiency and effectiveness.¹

Today, the U.S. Intelligence community includes the following:

- Central Intelligence Agency
- National Security Agency
- Defense Intelligence Agency
- National Geospatial-Intelligence Agency
- National Reconnaissance Office
- Intelligence elements of the Army, Navy, Air Force, Marine Corps
- The Federal Bureau of Investigation
- The Department of Energy
- The Department of the Treasury
- The Coast Guard
- Bureau of Intelligence and Research, Department of State

As recently as 1968 when Congress enacted Title II of the Omnibus Crime Control and Safe Streets Act of 1968, it established a protocol providing for search warrants in cases involving electronic surveillance for law enforcement purposes. Notably Congress included a provision clarifying that nothing in the act “shall limit the constitutional power of the President to take such measures as he deems necessary to protect the nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the

¹ 50 USC 401a(4)

security of the United States or to protect national security information against foreign intelligence activities.”²

Unfortunately, by the time of the Vietnam War and “Watergate,” a divergence between the Congress and the Presidency occurred as Congress became increasingly critical of the national intelligence effort. Leaders in the Congress like Senator Frank Church and Rep. Otis Pike led major investigations into intelligence activities and subsequently Congress pushed to establish clear divisions between the analytical and operational responsibilities within the CIA. Additionally Congress itself created the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence.

Throughout this pre-FISA period, the focus of concern was on domestic surveillance of U.S. citizens, not of foreign powers or agents, or of surveillance targets located outside the United States. The pre-FISA consensus was that the President's Constitutional powers in the area of foreign affairs were sufficient ground for his conducting foreign intelligence activities, including surveillance of non-U.S. citizens, without the need for special authorization by Congress to do so. The Supreme Court in *Katz v. United States*, 389 U.S. 347 (1967), for example, overturned the warrantless interception of a telephone conversation by a U.S. citizen as part of a criminal investigation as a violation of the Fourth Amendment. The Court specifically pointed out, however, that its decision in no way applied to the area of national security, stating that “[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving national security is a question not presented in this case.”

Five years later in 1972, the dispute between the Congress and the President over electronic surveillance would again go to the United States Supreme Court. In this case, the Supreme Court considered the question of whether the President, acting through the Attorney General, could conduct warrantless electronic surveillance of a U.S. citizen accused of bombing a CIA building. The Court held in *United States v. United States District Court*, 407 U.S. 297 (1972) (commonly known as the “*Keith*” case), that such “broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate application of Fourth Amendment safeguards” in the case of a domestic threat to national security. By focusing closely on the domestic aspects of the surveillance, the Court intentionally left open the question of whether the President had the power to conduct warrantless surveillance where “foreign powers or their agents” are involved, or where the surveillance target is outside the United States. The Court held only that, “prior judicial approval is required for the type of surveillance involved *in this case*,” i.e., surveillance of a U.S. citizen in the United States for the purpose of domestic intelligence gathering. The Court urged Congress to establish judicially-manageable standards for this type of surveillance within the United States.

In the context of foreign intelligence gathering, Court of Appeals decisions following *Keith* similarly declined to limit the President's power to conduct warrantless surveillance. In *United States v. Butenko*, 494 F.2d 593 (3rd Cir.), *cert. denied sub nom. Ivanov v. United States*, 419 U.S.

² 82 Stat. 214, formerly codified at 18 U.S.C. § 2511(3). The Supreme Court interpreted this provision not as a conferral or recognition of executive authority, but rather, an indication that Congress had “left presidential powers where it found them.” *United States v. United States District Court*, 407 U.S. 297, 303 (1972).

881 (1974), the Third Circuit held that warrantless electronic surveillance did not violate the Fourth Amendment if its primary purpose was to gather foreign intelligence. The Fifth Circuit likewise upheld the legality of a warrantless wiretap authorized by the Attorney General for foreign intelligence purposes where the conversation of an U.S. citizen was incidentally overheard. *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974). Consistent with the *Keith* Court's concern over the Fourth Amendment rights of U.S. citizens, the District of Columbia Circuit in 1975 held that a warrant was required for surveillance of a domestic organization that was neither an agent of a foreign power nor working in collaboration with a foreign power. *Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976).

These issues arose again during the Watergate scandal, when it was revealed in hearings before the Senate Committee to Study Government Operations with Respect to Intelligence Activities (widely known as the Church Committee) that the President used warrantless surveillance, including both electronic monitoring and physical searches, to gather information about U.S. citizens in the United States, including a Congressman, congressional staffers, anti-war protestors, and Martin Luther King, Jr. These hearings, along with the *Keith* Court's admonition to Congress, provided the impetus for what became FISA.

In 1978, Congress passed FISA, and President Carter signed it into law on October 25 that year, implicitly and dangerously conceding the pre-FISA view that the President's Constitutional powers themselves provided authority to conduct foreign surveillance activities, subject to the Fourth Amendment's application to domestic surveillance of U.S. citizens. The law established standards according to which the government could conduct electronic surveillance against a target in the United States for the purposes of collecting foreign intelligence, as opposed to information for the purposes of a criminal investigation. FISA identified foreign powers and their agents as the permissible targets of such electronic surveillance, and required the government to have probable cause to believe the target of FISA surveillance was an agent of a foreign power. The agent of a foreign power can be a U.S. person, and FISA defined a "U.S. person" as either 1. a U.S. citizen; 2. an alien lawfully admitted for permanent residence; 3. an unincorporated association a substantial number of which are U.S. citizens or permanent resident aliens; or 4. a U.S. corporation.

The law specified two ways in which the government could lawfully conduct such electronic surveillance. The first required a court order (a "FISA warrant") to authorize such surveillance, and FISA created the Foreign Intelligence Surveillance Courts ("FISC"), one at the district level to review applications for FISA warrants, and an one at the appellate level to review any governmental challenges to the denial of an application. The second permitted the government to conduct surveillance without a FISA warrant in emergency circumstances with the approval of the Attorney General, provided that the government applied for a FISA warrant within 24 hours of beginning the surveillance.

As originally enacted, FISA only regulated electronic surveillance as defined in the statute, not physical searches. More importantly, the law did not and was not intended to regulate any kind of surveillance of targets located outside the United States, and this lack of regulation was consistent with both the purpose of and impetus for the Act.

In 1995, Congress expanded FISA to cover physical searches to obtain foreign intelligence. Under the amended law, the government can conduct physical searches under a FISA warrant upon showing probable cause to believe that the target of the search is a foreign power or the agent of a foreign power, that the premises to be searched contains foreign intelligence information, and that the premises is owned, used, possessed by, or is in transit to a foreign power or the agent of a foreign power. The amended FISA also allowed the President to authorize for up to one year of any premises, provided that the Attorney General certifies to the FISC that the premises are exclusively controlled by a foreign power, and that there is no substantial likelihood that the search will involve the premises, information, material, or property of a U.S. person, as defined by FISA.

In 1998, Congress again amended FISA to allow the government to install and use pen registers and trap and trace devices to investigate international terrorism and clandestine intelligence activities. A pen register records all of the calls made from a specific number, while a trap and trace device records all calls made to a specific number (that is, a caller-id box is a trap and trace device). The 1998 amendments also extended this monitoring authority to include any type of electronic communication, including electronic mail. The amended FISA explicitly prohibited the use of such surveillance of U.S. persons for activities protected by the First Amendment.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA Patriot Act"), Public Law 107-56 (2001), signed into law on October 26, 2001, contained several amendments to FISA.

First, the Patriot Act amendments changed the certification federal officials are required to make to the FISA Court to obtain a FISA warrant. Under the amended FISA, the government must certify that a "significant purpose" of the electronic surveillance or physical search is the collection of foreign intelligence. This allows the government to obtain a FISA warrant in cases where a criminal investigation may also be a purpose of the surveillance. This change made clear that the so-called "wall" between criminal investigations and foreign intelligence gathering activities should not limit the power of the Executive to gather foreign intelligence information.

Second, the Patriot Act also amended FISA to allow for "multipoint" or "roving" electronic surveillance. As explained in the Conference Report on the Intelligence Authorization Act for Fiscal Year 2002, H. Rept. 107-328 at 24, this amendment "allows the FISA court to issue generic orders of assistance to any communications provider or similar person, instead of to a particular communications provider." In the absence of this amendment, a surveillance target could defeat investigative efforts by doing something as simple as changing cell phone providers, or using pay phones in different locations. This amendment allows the government to continue surveillance immediately if a FISA target changes providers or locations, rather than going back to the FISA Court to obtain a new warrant.

Third, FISA as amended by the Patriot Act provides that the government may apply for an order or extend an order authorizing or approving the installation of a pen register or trap and trace device, "for any investigation to protect against international terrorism or clandestine intelligence activities, provided such investigation of a United States person is not conducted solely on the

basis of activities protected by the first amendment to the Constitution." Additionally, the amendments allow the government to install and use such devices to track forms of electronic communication other than telephone calls, such as electronic mail.

The USA PATRIOT Improvement and Reauthorization Act of 2005, Public Law 109-177 (2006), further amended FISA to allow the government to apply for a FISA warrant for the "production of any tangible things...for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." Again, however, where such an investigation involves a United States person, the law states that government cannot proceed based solely on activities protected by the First Amendment.

The Protect America Act of 2007, Public Law 110-55 (2007), made several important amendments to FISA. First, it immunized non-governmental third parties like telecommunications companies from liability for providing information to the government pursuant to either a FISA warrant or a certification by the Attorney General or the Director of National Intelligence that the acquisition of the intelligence or the electronic surveillance being conducted is lawful and that the assistance requested is necessary.

There has been a substantial amount of litigation against telecommunications service providers for assisting the government prior to the Protect America Act's grant of immunity. The lead case is *Hepting v. AT&T*, filed in the United States District Court for the Northern District of California in 2006, in which the plaintiffs claim AT&T unlawfully assisted the government in collecting information about communications routed through AT&T's network. The ACLU has filed similar cases against AT&T and Verizon. The government intervened in the *Hepting* case, arguing that the case should be dismissed under the state secrets doctrine because AT&T could not mount a defense without revealing information related to any government certification or request for assistance pursuant to FISA. This is information the government does not have to disclose under FISA, because like revealing the existence of a FISA warrant or an application for one, such disclosure could hamper the government's foreign intelligence gathering activities. Nevertheless, the District Court rejected the government's arguments and ruled the case could go forward. The government appealed the decision to the Ninth Circuit, which heard arguments in August 2007 and has not yet issued its decision.

The most important amendment included in the Protect America Act, however, is a clarification of the scope of FISA itself. FISA originally proscribed the authority of the Executive to conduct electronic surveillance of foreign powers and agents of foreign powers acting within the United States, not targets located outside the country. This made sense, since the impetus behind FISA was the government's past use of electronic surveillance to monitor U.S. citizens in the United States, and Fourth Amendment implications of such activity. Since FISA's original enactment, however, changes in telecommunications technology, coupled with the law's definition of electronic surveillance as it existed circa 1978, effectively expanded the scope of the law to require a FISA warrant in cases involving surveillance of targets located in foreign countries, because such communications might at some point in their transmission be routed through the United States. The Protect America Act remedies this problem by clarifying that, "nothing in the

definition of electronic surveillance [in FISA] shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States."

These changes are consistent with the responsibilities of the President in matters involving national security, contemplated by the Constitution which provide a framework within which the government can conduct surveillance for the purpose of collecting foreign intelligence against targets located in the United States. The Protect America Act, however, is set to expire on February 5, 2008, and Congress has yet to pass legislation either reauthorizing its provisions or replacing them.

RESOURCES

Cases

United States v. United States District Court, 407 U.S. 297 (1972).

Katz v. United States, 389 U.S. 347 (1967).

Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976).

United States v. Butenko, 493 F.2d 593 (3rd Cir.), *cert. denied sub nom, Ivanov v. United States*, 419 U.S. 881 (1974).

United States v. Brown, 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974).

Statutes

50 U.S.C. sec. 1801 *et seq.* (Foreign Intelligence Surveillance Act).

Public Law 110-55 (2007) (Protect America Act of 2007).

Public Law 109-177 (2006) (USA PATRIOT Improvement and Reauthorization Act of 2005).

Public Law 107-56 (2001) (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001).