Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

March 10, 2020

Foreign Intelligence Surveillance Act (FISA): An Overview

Introduction

Congress enacted the Foreign Intelligence Surveillance Act (FISA) in 1978. FISA provides a statutory framework for government agencies to obtain authorization to gather foreign intelligence by means of (1) electronic surveillance, (2) physical searches, (3) pen registers and trap and trace devices (which record or decode dialing, routing, addressing, or signaling information), or (4) the production of business records and other tangible things. Agencies typically request authorization for such activities from the Foreign Intelligence Surveillance Court (FISC), a specialized court created by FISA to act as a neutral arbiter of agency requests for FISA orders.

FISA's History

Following revelations regarding widespread privacy violations by the federal government during the Watergate era, Congress enacted FISA to establish guidelines for government collection of foreign intelligence. FISA defines "[f]oreign intelligence information" as information relating to a foreign power or that generally concerns the ability of the United States to protect against international terrorism or a potential attack by a foreign power or agent of a foreign power. Though Congress initially limited FISA to regulating government use of electronic surveillance, Congress subsequently amended FISA to regulate other intelligence-gathering practices, such as physical searches, the use of pen registers and trap and trace devices, and compelling the production of certain types of business records.

Shortly after the 9/11 terrorist attacks, Congress enacted the USA PATRIOT Act (Patriot Act) to "provid[e] enhanced investigative tools" to "assist in the prevention of future terrorist activities and the preliminary acts and crimes which further such activities." Section 215 of the Patriot Act amended FISA to enlarge the scope of FISA's business records provision. Section 206 of the act authorized the government to seek "roving" wiretaps. And in 2004, Congress amended FISA to simplify the evidentiary showing necessary to obtain a FISA order to investigate non-U.S. persons suspected of engaging in international terrorism. All three provisions are temporary and have been reauthorized several times. Most recently, in late 2019, Congress extended all three provisions through March 15, 2020. Congress currently is considering whether to reauthorize these provisions again. If they are allowed to expire, grandfather clauses permit them to remain effective with respect to investigations that began, or potential offenses that took place, before the expiration date.

In the summer of 2013, news reports revealed that the National Security Agency (NSA) was engaged in the bulk collection of telephone metadata under Section 215 of the Patriot Act. In 2015, Congress enacted the USA FREEDOM Act, which circumscribed the government's ability to obtain telephone records as part of its foreign intelligence gathering operations.

Other major changes to FISA include the FISA Amendments Act of 2008 (FAA), codified as Title VII of FISA. These amendments established procedures governing the targeting—for intelligence-gathering purposes—of non-United States persons located abroad. They also established statutory and procedural protections regarding surveillance of U.S. persons located outside the United States. Congress last reauthorized Title VII of FISA in early 2018. Title VII will be up for reauthorization in 2023.

"Traditional" FISA

FISA Sections 1804, 1805, 1823, and 1824, otherwise known as the "traditional" FISA provisions, provide a framework by which government agencies must seek a FISA order to engage in surveillance or conduct physical searches for purposes of collecting foreign intelligence. Under FISA, federal officials seeking an order from the FISC must first obtain approval from the Attorney General, Acting Attorney General, Deputy Attorney General, or if designated, the Assistant Attorney General for National Security. They must then submit an application to the FISC.

FISC applications must include the following: (1) the applicant's identity if known; (2) information regarding the target's identity; (3) why the target may be searched or surveilled; (4) a statement establishing a sufficient relationship between the target and the search location; (5) a description of what will be searched or surveilled; (6) a description of the nature of the information sought or of the foreign intelligence sought; (7) proposed minimization procedures; (8) a discussion of how the search or surveillance will be carried out; and (9) a discussion of prior applications. If electronic surveillance is sought, applications must also discuss the duration of the surveillance.

FISC applications must be accompanied by written certifications from specified executive branch officials regarding the nature, purpose, and significance of the information to be sought. For the FISC to issue a FISA order, the government must show probable cause that the target of the surveillance is a foreign power or an agent of a foreign power, and that the target is using, or is about to use, the facilities or places at which the search or surveillance is directed.

Section 206

Section 206 of the Patriot Act amended FISA to permit multipoint, or "roving," wiretaps by adding flexibility to the

degree of specificity with which an applicant for a FISA order must identify the location or facility subject to electronic surveillance. Specifically, if the surveillance target is taking actions that "may have the effect of thwarting" surveillance (such as using disposable cell phone numbers or email addresses), the government may use a single FISA order to conduct surveillance on new phone numbers or email addresses used by the target without needing to apply to the FISC for a new order. However, the FISC must be notified within 10 days of the surveillance being directed at such new facilities.

Section 215

Section 215 of the Patriot Act enlarged the scope of materials that the government can seek under FISA to include "any tangible thing." Section 215 also eased the standard that an applicant must meet to obtain a FISA order compelling the production of "tangible thing[s]." Thus, an applicant for a FISA order must now provide "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to" a foreign intelligence, international terrorism, or espionage investigation.

Following the 2013 disclosure that the NSA had relied on Section 215 to engage in the bulk collection of telephone metadata, Congress amended Section 215 in the USA FREEDOM Act to require the use of a "specific selection term" (SST) to "limit collection to the greatest extent reasonably practicable." An SST was defined as "a term that specifically identifies a person, account, address, or personal device, or any other specific identifier." These amendments also prohibited the government from targeting Section 215 orders at broad geographic regions (such as a state or zip code) or at communications service providers (such as Verizon or AT&T).

Amended Section 215 established a slightly relaxed standard for obtaining telephone metadata on an ongoing basis in international terrorism investigations. Whereas a standard order under Section 215 would compel the production of only those records that are responsive to an approved SST, an order seeking telephone records for an international terrorism investigation can also be used to produce a second set of telephone records that are *connected* to one of the records that was directly produced by the SST. For example, if Alice called Bob, and Bob also called Charles, then a single Section 215 order that used Alice's phone number as an SST could obtain records of both Alice's call to Bob *and* Bob's call to Charles. In order to employ this process, the government must first demonstrate to the FISC that there is a "reasonable articulable suspicion" that the SST is associated with a foreign power, or an agent of a foreign power, who is engaged in international terrorism.

Section 6001(a) of the Intelligence Reform and Terrorism Prevention Act (IRTPA)

In 2004, Congress amended FISA as part of the Intelligence Reform and Terrorism Prevention Act (IRTPA) to change the rules regarding the types of individuals who may be targets of FISA-authorized searches. Also known as the "lone wolf" provision, Section 6001(a) of the IRTPA permits surveillance of non-U.S. persons who are shown to be engaged in international terrorism, but without requiring evidence linking those persons to an identifiable foreign power or terrorist organization.

FISA Amendments of 2008

Title VII of FISA, added by the FAA, establishes additional procedures to acquire foreign intelligence information regarding persons who are believed to be outside of the United States. These provisions affect both U.S. persons as well as non-U.S. persons, and are scheduled to sunset in 2023.

The FAA added Section 702 of FISA, which establishes procedures to collect foreign intelligence when communications travel through the United States' communications infrastructure. Under Section 702, the government may compel the assistance of electronic communications service providers for a period of up to one year in targeting non-U.S. persons reasonably believed to be located outside the United States. The Attorney General (AG) and the Director of National Intelligence (DNI) must jointly certify that they authorize any such targeting, and the FISC must approve any program under Section 702 before its implementation. If time does not permit submitting the requisite certification to the FISC before authorization, the AG and DNI must submit their certification to the FISC within seven days of the commencement of the surveillance.

The FAA also added Sections 703 and 704 of FISA, which regulate other aspects of foreign intelligence collection. Section 703 grants jurisdiction to the FISC to "review an application and to enter an order approving the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information." Section 704 mandates that, subject to certain exceptions, the government must obtain a FISA order to target a U.S. person located abroad when the government also would have had to obtain a warrant to conduct domestic surveillance of that person.

Joshua T. Lobert, Legislative Attorney

IF11451

Disclaimer