Confrontation or Collaboration?

Congress and the Intelligence Community

Electronic Surveillance and FISA

Eric Rosenbach and Aki J. Peritz

HARVARD Kennedy School
JOHN F. KENNEDY SCHOOL OF GOVERNMENT

Belfer Center
for Science and International Affairs

Electronic Surveillance and FISA

Electronic surveillance is one of the core methods the Intelligence Community (IC) utilizes to gather information on foreign adversaries and terrorist organizations. Public revelations that President Bush authorized the National Security Agency (NSA) to perform electronic surveillance on electronic communications with a domestic nexus, without a court-issued warrant, resulted in significant debate about the means, legality and effectiveness of electronic surveillance.

This memo provides an overview of electronic surveillance and discusses the recent debate in Congress about and the Foreign Intelligence Surveillance Act (FISA).

What is Electronic Surveillance?

Electronic surveillance refers to the acquisition of the contents of wire, radio and other electronic communications. Electronic surveillance has emerged as a critical tool for detecting and intercepting international terrorists within the United States and overseas.

Legal Basis for Electronic Surveillance

There are two main frameworks for electronic surveillance. One, based on Title III of the U.S. Code, covers surveillance in the investigation of serious domestic crimes. The second, based on FISA, covers foreign intelligence surveillance and serves as the main tool for electronic surveillance of international terrorists.

Congress passed FISA in 1978 in the wake of revelations that the White House authorized warrantless surveillance of Americans. In brief, the legislation stated:

- FISA would be the "exclusive means" governing the use of electronic surveillance in international terrorism and other foreign intelligence investigations.
- The Federal Bureau of Investigation (FBI) and NSA would serve as the lead agencies to gather foreign intelligence relevant to the FISA framework.
- The IC would work through the Foreign Intelligence Surveillance Court (FISC) to secure a warrant before undertaking foreign intelligence surveillance of a domestic nature.

Following 9/11, Congress and the White House agreed the IC needed greater flexibility to address the threat posed by international terrorism. Congress therefore passed amendments to the FISA legislation in the USA-PATRIOT Act in 2001. The USA-PATRIOT Act significantly eased the standard required of a federal officer to apply for intelligence collection under the FISA framework. Congress also adjusted and modernized FISA in the Protect America Act of 2007 and the FISA Amendments Act of 2008.

How FISA Works

Intelligence agencies do not need a warrant to collect information on foreign adversaries and terrorists with communications that occur outside the United States. When electronic communications either transit or occur within the United States, however, intelligence officials must use FISA. In sum, a *significant purpose* of the electronic surveillance must be to obtain intelligence in the U.S. on foreign powers (such as enemy agents or spies) or individuals connected to international terrorist groups.

- To use FISA, the government must show probable cause that the "target of the surveillance is a foreign power or agent of a foreign power."

Civil Liberties Protections

Under FISA, U.S. citizens, legal residents and U.S. corporations (known as "U.S. persons") are protected against illegal search and seizure by the Fourth Amendment; hence, FISA includes a number of provisions to protect civil liberties. Furthermore, FISA also explicitly states that, "no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the First Amendment of the Constitution of the United States."

While surveillance of U.S. persons is permitted under FISA, the IC must "minimize" the collection of information not directly applicable to the intended target.

- These strict minimization procedures require the IC to obscure the identity of any protected communications incidentally captured as part of the surveillance.
- Unlike Title III criminal warrants, however, minimization occurs after collection under FISA.

Controversy Regarding Electronic Surveillance

In December 2005, the *New York Times* revealed that President Bush authorized the NSA to conduct a warrantless surveillance program. The White House stated that the program targeted the international communications of individuals connected to al-Qaeda or other foreign terrorist organizations. Skeptics of the program feared that the President had overstepped the bounds of his authority and spied on Americans. The surveillance activities became known as either the "Terrorist Surveillance Program" (TSP) or "warrantless wiretapping."

As reports of the electronic surveillance efforts gradually became public, some argued the program was necessary to intercept al-Qaeda-related communications more quickly than the FISA process allowed. They claimed that the process for obtaining FISA warrants for each individual target prevented the government from obtaining this data in a timely fashion.

As questions about the legality of the surveillance program grew, proponents argued that:

- The President could legally ignore FISA because he possessed the inherent authority to conduct warrantless surveillance for intelligence purposes as part of his constitutional Article II powers as Commander in Chief.
- The Congressional Authorization for Use of Military Force (AUMF) of September 18, 2001 provided authority for the President to take these actions.

On the other hand, others argued the President could not completely bypass the FISA process because Congress explicitly intended FISA to be the "exclusive means" for authorizing this type of surveillance.

- This perspective indicated that the AUMF was not intended to cover electronic surveillance, particularly since Congress passed the USA-PATRIOT Act to amend various parts of FISA almost immediately after it passed the AUMF.
- Furthermore, some argued the program offered too few protections to prevent the government from monitoring the communications of innocent Americans and lacked appropriate congressional oversight.

In January 2007, Attorney General Alberto Gonzales informed Congress that the FISC had issued orders authorizing the collection of international communications into or out of the United States when the government had probable cause to believe that the communications belonged to a terrorist organization. Gonzales noted that because of the FISC order, the President would discontinue his authorization of TSP and conduct all electronic surveillance under FISA.

FISA Modernization

Although debate about the legality of the TSP continued, most members of Congress agreed that technological evolutions required "modernization" of the FISA legal framework.

One reason for updating the law was that the telecommunications industry had evolved significantly since the inception of FISA in 1978. Most importantly, a large portion of international communications moved from satellites, which are "radio" communications under FISA, to fiber-optic cables, which are "wire" communications under FISA. The original law did not regulate international radio communications unless the government targeted a U.S. person.

- FISA originally regulated international wire communications only when the surveillance was conducted in the U.S. Since a significant portion of the global fiber-optic network currently passes through the U.S., the government argued that FISA should be modified to allow for foreign intelligence surveillance of non-U.S. persons from within the country.

Nevertheless, there was concern that attempts to modernize FISA risked weakening civil liberties protections by removing the individualized warrant requirement that underpinned the original FISA law. Some believed that program warrants and longer periods of emergency warrantless surveillance could have further undermined the intent of original protections.

- Some argued the "communications revolution" argument was overblown. The shift of international communications that from satellites to fiber should not impact the FISA review process.
- Some also saw in FISA modernization a way to facilitate additional 'backdoor' intelligence gathering practices, such as large-scale data mining.

The FISA Amendments Act of 2008

While a number of FISA-related issues remain for Congress to resolve in the future, the FISA Amendments Act of 2008 (set to expire in 2012) addressed the following issues:

- FISA and Title III remain the *exclusive means* for conducting electronic surveillance.
- In order to conduct electronic surveillance of U.S. persons located outside the country, the government must now go through the FISA court order process; previously, the Attorney General could certify this collection under an executive order.
- A provision permits greater use of "program warrants" in order to target broad groups of foreign targets, as opposed to more individualized ones.
- The Attorney General has an extended period during which he can approve surveillance without a warrant in emergency situations.
- Congress granted telecommunications service providers immunity from prosecution for cooperating with government surveillance programs, as long as they received written government assurances about the legality of their cooperation from the government.
- Relevant Senate and House committees will receive from the Attorney General a semi-annual report on FISA-based targets.
- Congress included a number of added oversight and reporting requirements in order to play a more active role in reviewing the government's use of FISA.

Electronic Surveillance Developments

June 1934 1934

Congresses passes the Federal Communications Act, the first legislation regarding the use of wiretaps.

June 1968 1968

Congress passes the Omnibus Crime Control and Safe Streets Act, which includes the first federal legislation restricting the use of wiretaps in an effort to "safeguard the privacy of innocent persons."

1975 1975

A Senate Committee, headed by Senator Frank Church, investigates illegal activity on the part of the FBI and CIA, including the use of warrantless wiretaps against anti-war and civil rights leaders.

1940 1950 1960 1970

December 1967 1967

The Supreme Court extends Fourth Amendment protections in Katz v. United States, ruling that the government must obtain a warrant before initializing wiretaps and that warrants must be limited in scope and duration. The Court, however, allows for exceptions in cases involving national security.

July 1974 1974

The House Judiciary Committee issues articles of impeachment against President Richard Nixon in part for his authorization of illegal wiretaps against U.S. citizens.

October 1978 1978

Responding in part to the Watergate scandal and the Church Committee findings, Congress passes the Foreign Intelligence Surveillance Act (FISA) and creates the Foreign Intelligence Surveillance Court.

Electronic Surveillance

October 1986 1986

Congress passes the Electronic Communications Privacy Act to restrict electronic surveillance on new technologies, including computers, cell phones, and pagers.

December 2005 2005

The New York Times first reports on the NSA's "Terrorist Surveillance Program."

February 2008 2008

PAA expires under its sunset clause, requiring Congress to once again deliberate and construct an effective amendment to FISA.

1980 1990 2000 2010

October 2001 2001

President George W. Bush signs the USA-PATRIOT ACT into law, which among other measures streamlines the process of obtaining warrants to conduct surveillance and amends FISA to allow surveillance to cover people, rather than individual devices.

August 2007 2007

President Bush signs the Protect America Act of 2007, legalizing some forms of warrantless surveillance and to account for technological advancements since the passage of FISA in 1978.

July 2008 2008

Congress passes the FISA Amendments Act, which includes immunity for all telecommunication companies and eases restrictions on surveillance of targets outside the United States.

e Developments

Sources

Electronic Surveillance and FISA

Bazan, Elizabeth B. The Foreign Intelligence Surveillance Act: Comparison of the Senate Amendment to H.R. 3773 and the House Amendment to the Senate Amendment to H.R. 3773, 12 June 2008. Accessed 19 March 2009 <http://www.fas.org/sgp/crs/intel/RL34533.pdf>.

Congressional Record (House) 20 June 2008. 19 March 2009. <http://www.fas.org/irp/congress/2008_cr/house-fisa.html>.

Congressional Record (Senate) 9 July 2008. FISA Amendments Act of 2008, 19 March 2009 <http://www.fas.org/irp/congress/2008_cr/fisa070908.html>.

Hess, Pamela (2008-06-20). "House immunizes telecoms from lawsuits". Washington Times 20 June 2008. Accessed 19 March 2009 <http://www.washingtontimes.com/news/2008/jun/20/house-immunizes-telecoms-from-lawsuits>.

Liptak, Adam. "U.S. Defends Surveillance to 3 Skeptical Judges." New York Times. 16 August 2007.

Lowenthal, Mark. Intelligence: From Secrets to Policy. 4th ed. Washington, D.C.: CQ Press, 2009.

Risen, James and Eric Lichtblau. "Bush Lets U.S. Spy on Callers Without Courts." New York Times. 16 December 2005.

"H.R.3162: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Enrolled as Agreed to or Passed by Both House and Senate)" Library of Congress. <http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:>.