The Heritage Foundation
LEADERSHIP FOR AMERICA

ISSUE BRIEF

No. 3732 | SEPTEMBER 18, 2012

Foreign Intelligence Surveillance Amendments Act of 2008 Set to Expire

John G. Malcolm

Last Wednesday, the House of Representatives reauthorized the Foreign Intelligence Surveillance Amendments Act of 2008 (FAA), which expires at the end of the year. The Senate will take up the measure shortly. James Clapper, the Director of National Intelligence (DNI), and U.S. Attorney General (AG) Eric Holder have informed leaders in Congress that reauthorizing the FAA is "the top legislative priority of the national Intelligence Community," and national security officials from the previous Administration have testified in favor of reauthorization.[1]

FAA Remedied Defects in FISA. Enacted in 1978, the Foreign Intelligence Surveillance Act (FISA) created a secret national security court to review wiretap applications for national security investigations conducted in the U.S. that involve foreign powers or their agents.[2] With FISA, Congress recognized the need to distinguish between rigorous judicial review of intelligence surveillance efforts in the U.S. (where the Fourth Amendment applies) and allowing the government to conduct surveillance overseas (where the Fourth Amendment does not apply) without judicial oversight.[3]

These distinctions were made through the definition of "electronic surveillance." However, modern technology resulted in an increasing number of calls and e-mails passing through the U.S. in which it was not immediately clear that both ends of the communications were occurring outside the U.S. The government then expended significant manpower generating FISA Court applications for surveillance against persons outside the U.S., even though Congress meant to exclude these targets when it enacted FISA.

The 2008 amendments to FISA addressed this by allowing the FISA Court to streamline approval for surveillance of suspected foreign state and terrorist agents without requiring an individualized application for each target as long as the government reasonably believes the targets are located outside the U.S. Individual warrants are still required if the target is a U.S. citizen, regardless of where he is located and even if the government believes he is acting as a foreign agent.[4]

This streamlined process requires the AG and the DNI to provide an annual certification to the FISA Court identifying the categories of foreign intelligence targets subject to surveillance and certifying that all FAA requirements—including targeting and minimization procedures—have been met. The "targeting procedures" are rules to determine whether each target is located outside the U.S. and are designed to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."[5] The "minimization procedures" require that surveillance be "reasonably designed...to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons."[6]

Further, the FAA prohibits "intentionally target[ing] a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States."[7]

This paper, in its entirety, can be found at **http://report.heritage.org/ib3732**

Produced by the Center for Legal & Judicial Studies

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

This prevents the surveillance of foreign targets as a pretext to conduct surveillance of people within the U.S. The certification must state that the guidelines adopted to ensure FAA compliance are consistent with the Fourth Amendment and that "a significant purpose of the acquisition is to obtain foreign intelligence information."[8]

FAA Provides Adequate Protections and Oversight. The FAA also created various levels of oversight—more than exist with respect to domestic wiretaps—to ensure compliance. The AG must adopt guidelines to ensure that surveillance is not used against non-qualifying targets, and the AG and DNI must provide semiannual assessments of compliance to Congress and the FISA Court.

The Inspectors General of the Justice Department and participating intelligence agencies may conduct implementation reviews and must provide the results to Congress. Meanwhile, each intelligence agency must conduct an annual compliance review and provide the results to the FISA Court and the Intelligence and Judiciary Committees of Congress. Additionally, as the government stated in its brief before the U.S. Supreme Court in *Clapper v. Amnesty International USA*:

> If the government intends to use or disclose any information obtained or derived from its acquisition of a person's communications under Section 1881a in judicial or administrative proceedings against that person, it must provide advance notice of its intent to the tribunal and the person, whether or not the person was targeted for surveillance under Section 1881a.... That person may then challenge the use of that information in district court by challenging the lawfulness of the Section 1881a acquisition.[9]

Inadvertent Monitoring. Senator Ron Wyden (D–OR) is currently blocking FAA reauthorization because the government has not provided an estimate of how many conversations involving Americans have been inadvertently intercepted. It is inescapable, however, that authorities who have been authorized to monitor the communications of a target will occasionally intercept communications from non-targets.

This is the case regardless of whether the individual whose communications are being monitored is the target of a domestic criminal investigation or a national security operation. After all, those who are monitoring the conversations have no idea who the target is going to call, and vice versa.

If a suspected drug dealer being monitored calls a restaurant to place an order, an agent will listen to that call until he or she determines the conversation has nothing to do with a drug transaction, at which point the agent will stop listening. Incidental collections such as this also occur when intelligence agents monitor the phone calls and e-mails of suspected terrorists overseas.

Just as it is not possible ahead of time to identify every restaurant host or auto mechanic whose conversation with a suspected drug dealer gets intercepted in a domestic criminal investigation, the same is true for overseas national security investigations. These are further complicated by the difficulty of identifying the nationalities of all participants in a communication with an overseas target. On the other hand, an American who is not a target of our surveillance efforts might end up participating in a relevant communication with a foreign target located outside

1. Eric H. Holder, Jr., U.S. Attorney General, and James R. Clapper, Director of National Intelligence, letter to Speaker John Boehner, Senate Majority Leader Harry Reid, House Minority Leader Nancy Pelosi, and Senate Minority Leader Mitch McConnell, Feb. 8, 2012, http://intelligence.senate.gov/pdfs112th/dni_ag_letter.pdf (accessed September 17, 2012); and Kenneth L. Wainstein "Statement Concerning the Reauthorization of the FISA Amendments Act," testimony before the Subcommittee on Crime, Terrorism and Homeland Security, Committee on Judiciary, U.S. House of Representatives, May 31, 2012, http://judiciary.house.gov/hearings/Hearings%202012/Wainstein%2005312012.pdf (accessed September 17,2012).
2. 50 U.S.C. § 1803(a).
3. See *United States v. Verdugo-Urquidez* (1990).
4. 50 U.S.C. § 1881.
5. 50 U.S.C. § 1881a(g)(2)(A)(i).
6. 50 U.S.C. §§ 1801(h)(1), 1821(4)(A).
7. 50 U.S.C. § 1803(b)(2).
8. 50 U.S.C. § 1881a(g)(2)(A)(iii)-(vii).
9. Brief for Petitioners at 8, Clapper v. Amnesty International USA, No. 11-1025, *available at* http://www.americanbar.org/content/dam/aba/publications/supreme_court_preview/briefs/11-1025_petitioner.authcheckdam.pdf.

the country, in which case that communication could be monitored as relevant "foreign intelligence information."

The intelligence community cannot estimate the number of U.S. persons whose communications have been intercepted—inadvertently or otherwise—under the FAA. This should hardly be surprising. It was inevitable, as with any wiretap, that the incidental collection of communications involving non-targeted U.S. persons would occur and that records of non-relevant communications would not be maintained, given the limits of technology and collection methods. Further, any disclosure of the content of those communications would likely violate the privacy rights of the affected individuals.

Enabling the Collection of Critical Intelligence. Robert Litt, General Counsel for the Office of the DNI, recently stated: "I know of specific instances, both involving terrorist attacks and involving other kinds of threats, where we have been able to thwart them or gain significant insight into them as a result of this collection activity."[10] Senator Dianne Feinstein (D–CA), Chairwoman of the Senate Intelligence Committee, stated that the government has implemented the FAA's "surveillance authorities in a responsible manner with relatively few incidents of non-compliance. Where such incidents have arisen, they have been the inadvertent result of human error or technical defect and have been promptly reported and remedied."[11]

The FISA Amendments Act enables our intelligence community to gather critical information about our determined adversaries, who still actively plot to attack our country, with minimal risk of unwarranted invasions of privacy. The protections in existing law are sufficient to prevent abuse, and Congress should not deny the Executive the tools necessary to investigate and prevent potential future acts of terrorism.

*—**John G. Malcolm** is a Senior Legal Fellow in the Center for Legal & Judicial Studies at The Heritage Foundation.*

10. Siobhan Gorman, *President Pushes to Extend Surveillance Law*, Wall St. J., Sept. 12, 2012.
11. S. Rep. No. 112-174, at 7 (2012), *available at* http://www.gpo.gov/fdsys/pkg/CRPT-112srpt174/pdf/CRPT-112srpt174.pdf.