

FISA AMENDMENTS ACT OF 2008

OVERVIEW

The FISA Amendments Act of 2008 provides critically important authority for the U.S. Intelligence Community to acquire foreign intelligence information by targeting foreign persons reasonably believed to be outside the United States. It ensures that the Intelligence Community has the flexibility and agility it needs to identify and respond to terrorist and other foreign threats to our security.

Consistent with current FISA, the Act provides a key role for each branch of Government. It assigns responsibilities jointly to the Attorney General (AG) and the Director of National Intelligence (DNI) to ensure that the Nation's chief law enforcement and intelligence officials work together in collecting foreign intelligence in accordance with the law. It requires the Foreign Intelligence Surveillance Court (FISA Court) to review and approve, or order modifications to, the procedures required by the Act and to ensure that those procedures are consistent with the Fourth Amendment to the Constitution. And it requires that information about the implementation of these new procedures be reported to Congress, to ensure that Congress can fulfill its oversight role.

PRIVACY AND CIVIL LIBERTY PROTECTIONS FOR AMERICANS

Exclusivity. The Act reiterates the exclusive means provision from the 1978 FISA statute and requires express statutory authorization for electronic surveillance conducted outside of FISA and specific chapters of Title 18, United States Code.

Targeting Procedures. The targeting procedures are designed to ensure that only persons reasonably believed to be outside the United States will be targeted under these authorities. At least annually, the AG and DNI must submit to the FISA Court for review and approval targeting procedures for making that fundamental determination.

Minimization Procedures. Under FISA and Title 18, law enforcement and the Intelligence Community use minimization procedures to protect innocent conversations of Americans. Similarly in this Act, minimization procedures are instrumental in ensuring that information that is acquired about Americans, in the course of targeting foreigners, is used only for proper intelligence or law enforcement purposes. These procedures must be reviewed and approved at least annually by the FISA Court.

Individual Judicial Orders for Surveillance of Americans. The Act requires individual FISA Court orders based on probable cause for targeting Americans, not only when they are inside the U.S. but also, for the first time, when they are outside of the United States.

Reverse Targeting Guidelines. The Act requires adoption by the Attorney General and submission to the Congress and FISA Court of guidelines to ensure compliance with the Act's limitations, including its prohibition on reverse targeting.

TIMING OF COLLECTION AND JUDICIAL REVIEW

Timing of Judicial Review. The Act requires that the targeting procedures shall be submitted to and approved by the FISA Court before the collection begins.

Exigent Circumstances. If intelligence important to the national security may be lost or not timely acquired, collection can begin before the FISA Court reviews and approves the targeting procedures. The AG and DNI must submit the procedures within 7 days and the court would make a determination within 30 days. During this period, all relevant minimization and reverse targeting guidelines would apply.

LIABILITY PROTECTIONS AND OBLIGATIONS OF AMERICAN COMPANIES

Prospective Immunity. Private partners that act in accordance with orders, certifications, or directives provided under the law shall be protected against future liability.

Retroactive Immunity. The Act provides standards and procedures for liability protection for electronic communication service providers who assisted the Government between September 11, 2001 and January 17, 2007, when the President's Terrorist Surveillance Program was brought under the FISA Court.

A district court hearing a case against a provider will review, under a "substantial evidence" standard, the Attorney General's certification that certain providers either did or did not assist with the TSP. In making that determination, the court will have the opportunity to examine the highly classified letters to the providers that indicated the President had authorized the activity and that it had been determined to be lawful. The plaintiffs and defendants will have the opportunity to file public briefs on legal issues and the court should include in any public order a description of the legal standards that govern the order.

The immunity provision of the Act does not apply to any actions against the Government or Government officials.

OVERSIGHT AND ACCOUNTABILITY

Inspector General Review. The Act directs the Inspectors General of the Department of Justice, the Office of the DNI, the National Security Agency, and the Department of Defense to complete a comprehensive review, within the oversight authority of each IG, of the President's Terrorist Surveillance Program. In no later than a year, the Inspectors General shall submit a report to Congress; the report shall be unclassified but may include a classified annex.

Multiple Levels of Oversight. The Act provides for multiple levels of oversight both within the Executive Branch, including by Department of Justice and Intelligence Community Inspectors General, and in regular reporting to both the Congress and the FISA Court.

Sunset. The Act will sunset at the end of 2012.