Insight

Re-authorizing FISA: Options for Reform

JOSHUA LEVINE, JOHN BELTON | DECEMBER 6, 2023

Executive Summary

- The Foreign Intelligence Surveillance Act (FISA) requires re-authorization at the end of the year, prompting a handful of proposals to reform the current legislation to strengthen oversight and accountability, and to prevent warrantless querying of data that could belong to U.S. citizens.
- This paper briefly reviews the key reform issues, and focuses on the strongest of these vehicles, the Government Surveillance Reform Act (GSRA) of 2023 to re-authorize and reform FISA and other laws related to foreign intelligence and surveillance.
- The GSRA would institute reforms such as requiring intelligence agencies to get a warrant to acquire information that includes U.S. persons or purchase data from data brokers; increasing the presence of *amici curi*ae in hearings before the FISA courts; and setting new monitoring and reporting rules for information collected and used by intelligence agencies and law enforcement.

Introduction

The Foreign Intelligence Surveillance Act (FISA) of 1978 – a law that allows for the National Security Agency (NSA) to conduct surveillance on foreign agents and adversaries –- is set to expire at the end of 2023. Members of Congress are considering a few paths to reauthorization. One path, proposed by Senators Mark Warner and Marco Rubio and supported by 13 lawmakers, would re-authorize FISA for twelve years with limited reforms, specifically focused on the Federal Bureau of Investigation's (FBI) ability to query information collected under the law. Another path is the Protect Liberty and End Warrantless Surveillance Act, proposed by Representative Andy Biggs and a bipartisan group of lawmakers on the House Judiciary Committee, including Chair Jim Jordan and Ranking Member Jerrold Nadler. The bill would re-authorize FISA for three years, reform Section 702 querying procedures, limit the use of information collected under 702 by law enforcement without a warrant, require reforms to the FISA court, and prevent law enforcement from purchasing any data from third party data brokers. The final path is a bipartisan, bicameral proposal co-sponsored by 26 lawmakers called the Government Surveillance Reform Act (GSRA). This bill would re-authorize FISA for four years while imposing wide-reaching reforms to the government's surveillance authority because of concerns of potential abuses under authority. These reforms would impact FISA as well as Executive Order 12333 (EO 12333), which ensures the intelligence community (IC) can provide adequate information to the executive branch on foreign intelligence threats, and the Electronic Communications Privacy Act of 1986 (ECPA), which sets rules related to digital data collection surveillance by the IC and law enforcement, respectively.

The GSRA reforms are wide-ranging, including new warrant requirements when querying data that includes information on U.S. persons or purchasing data from third parties, as well as expanding reporting requirements for data obtained through FISA, EO 12333, or ECPA authority. Critical pieces of the legislation – including *amici curiae* reforms – have already passed the Senate in previous reform efforts.

While the GSRA targets specific components of government programs, the legislative intent is consistent: protecting U.S. persons from surveillance abuses by the government. FISA is an important tool for intelligence agencies and law enforcement, but evidence illustrates how these powers can be used improperly. This insight provides brief summaries of FISA, EO 12333, and the ECPA; analyzes some of the GSRA's key reforms; and discusses some of the potential implications of such reforms.

Existing Authorities: FISA, Executive Order 12333, and the ECPA

FISA

FISA enables U.S. intelligence services to conduct wide-reaching surveillance on foreign adversaries. The law, enacted in 1978, codifies intelligence agencies' powers to monitor foreign threats and provides oversight of the agencies' actions against U.S. persons. FISA's creation was most notably amended in 2008 to include Title VII, which codifies the authority provided to U.S. intelligence services over electronic and other surveillance tools for the digital age. Under Section 702, the National Security Agency (NSA) is responsible for collecting e-mails and internet communications and can also query them, while other intelligence and law enforcement agencies can only query the data.

Executive Order 12333

EO 12333 is intended to ensure the intelligence community can provide the executive branch with necessary information to protect the United States from foreign security threats in a timely manner. Originally issued by President Reagan, the EO permits agencies involved in gathering intelligence to collect information related to foreign communications or the communications of foreign nationals to combat terrorism. EO 12333 has raised similar concerns as 702, specifically that U.S. citizens' communications can be collected by the government without a warrant. Congressional testimony by former NSA Director Keith Alexander raised the possibility that the EO's "Special Procedures" section allows intelligence agencies to collect information that could be used to "map" Americans' social networks without a warrant.

ECPA of 1986

The ECPA was passed in 1986 to expand rules related to surveillance and information gathering to the emerging world of electronic communications, such as e-mail. The ECPA attempts to balance individuals' electronic privacy without inhibiting law enforcement's ability to pursue malicious actors. For example, accessing information stored on a home computer requires a warrant, but accessing an e-mail stored on a third-party server only requires a subpoena. Changes in data storage and the volume of data have created an environment where U.S. persons' private communications can now be accessed by government agents without a warrant.

Key Reforms of the GSRA

The reforms focus on requiring intelligence agencies to get a warrant if they are collecting information that includes U.S. citizens' data, including from third-party data brokers; reforming internal processes of the FISA courts and creating guardrails for the methods intelligence agencies employ for monitoring, storing, and reporting on information that would include or implicate U.S. persons.

Warrant Requirements for Queries, Collection, and Use of Information on U.S. Persons

The GSRA would prohibit law enforcement from querying any information collected under 702, EO 12333, or the ECPA on, or that is reasonably believed to implicate, a U.S. citizen or a person located in the United States if this would require a warrant in a domestic context. For the ECPA, a warrant would be required to collect and/or query location data, communications, and metadata, as well as phone and app-based call and texting records. Any information that is queried cannot be used for any purpose outside of the specific context for which the information was queried, including criminal, civil, or administrative proceedings.

Reforms for Data Brokers

This reform targets the "data broker loophole" – the process of government agencies purchasing commercially available information from data brokers to circumvent warrant requirements in the ECPA. Recent reports have identified several agencies as buyers, including the Department of Homeland Security, the Internal Revenue Service's Criminal Investigations Division, and the Defense Intelligence Agency, as well as the Federal Bureau of Investigation. This ban on commercially available information applies to all law enforcement agencies including at the state and local levels.

Amici Curiae and FISC Reforms

The GSRA expands the *Amici Curiae* program for the Foreign Intelligence Surveillance Court (FISC), initially implemented in 2015 to reduce the *ex parte* nature of the court. Currently, the program allows for the appointment of an *amicus curiae* only when there is a "novel or significant" interpretation of the law –restricting the number of appointees to 29 on a total of 6078 surveillance orders. By expanding the situations in which an *amicus curiae* can be appointed, it ensures there is a party present at FISC hearings responsible for advocating for U.S. persons' civil liberties.

Technical Assistance From Electronic Communication Service Providers

If the GSRA is adopted, under 702, the U.S. Attorney General (AG) or Director of National Intelligence (DNI) would be prohibited from directing technical assistance from electronic communication service providers (ECSP), such as telecommunications or technology firms, without demonstrating such assistance is necessary, narrowly tailored, and would not impose an undue burden on other users of the ECSP. Further, the ECSP is free to deny technical assistance unless the AG or DNI has a warrant that explicitly describes the assistance to be provided. This attempts to remove the incentive for the federal officials to pressure firms to disclose user information without a warrant, protecting users' privacy and potentially limiting jawboning by government agents.

Rules for Storing and Retaining Information on U.S. Persons

The GSRA would set data retention rules and requirements for accessing collected information and clarify rules related to acquiring or deleting private individuals' digitally stored information. The bill requires the AG and heads of intelligence agencies to develop and institute guidelines to limit retention and require deletion of information that could include Americans' data within five years of collection, unless the AG determines such information is directly necessary for an ongoing proceeding. Further, the bill would require consistent rules for all types of personal data that could be collected, including communications metadata, geolocation data, data held by interactive computer services (digital platforms and apps), and minimization standards that must be issued within 180 days of the bill's enactment.

Updated Reporting and Oversight Requirements

Beyond creating new requirements and restraints on data collection, the GSRA would impose new reporting requirements for agencies collecting, querying, and storing data related to foreign intelligence investigations. Annual reports detailing the subject matter of certifications granted under covered surveillance authority, statistics on the number of persons and identifiers targeted, and directives issued by communication type would be required from the director of the administrative office of the U.S. courts, the DNI, and the U.S. AG. The bill would also require reports investigating the quantity of national security directives, a risk assessment by the Inspector General, and the use of FISA authorities impacting protected activities and classes, such as organizations and activities protected by the First Amendment.

Potential Impact of Reforms

The GSRA also represents an attempt to address prior intelligence community abuses – including the improper querying of a member of Congress, "backdoor" searching of U.S. persons' conversations, and the use of FISA tools for analysts' personal inquires. To that end, the legislation would attempt to close many of the loopholes and statutory gaps used by the IC to monitor and collect domestic records. Many of these abuses were identified through previously mandated disclosures and compliance programs, showing Congress and Americans *ex post* the status of FISA authorized programs. The GSRA would attempt to continue the trend of increasing oversight and compliance requirements, implementing more granular and frequent disclosures, and providing a check on foreign intelligence operations that could unduly implicate U.S. citizens.

The GSRA's reforms related to digital surveillance are noteworthy because of changes in technology and the significant expansion in the amount of data created by and about individuals. This is important considering the expansion of internet-of-things devices across sectors and the general trend of more devices connecting with one another, which creates new opportunities for data collection and sharing, particularly with third parties, such as data brokers. By modernizing the legislation, the GSRA would bring current practices for collecting and querying communications metadata and geolocation data in line with more traditional sources, such as wiretapping, to help ensure that civil liberties are protected as technology evolves.

Beyond the immediate implications for government surveillance activities, the GSRA could pave the way for future actions related to digital privacy. The GSRA's focus on the government's use of data could create a lane for lawmakers to focus specifically on rules governing commercial use and markets for consumer data. Further, the GSRA could help ease tensions between the United States and counterparts abroad, particularly in Europe, where previous data sharing agreements have been dissolved due to a lack of guardrails around the IC's data collection and surveillance.