[INSERT “A” - PREPARED BY LEG. COUNSEL]

Table of Contents

Purpose and Summary

H.R. 6570, introduced by Rep. Andy Biggs (R-AZ), reauthorizes Section 702 of the Foreign Intelligence Surveillance Act (FISA) for three years with significant reforms. It requires the government to obtain an order from the Foreign Intelligence Surveillance Court (FISC) or a warrant prior to conducting U.S. person queries of information collected through Section 702. It provides for greater scrutiny of applications submitted to the FISC, increases transparency in surveillance applications, requires more frequent and detailed reports and audits, and establishes additional penalties for government employees who violate FISA or mislead the FISC.

The bill also closes the legal loophole that allows data brokers to sell Americans' personal information to law enforcement, intelligence agencies, and other government agencies without the agency first acquiring a warrant. If the agency were to gather this information itself, it would be required to obtain a warrant, subpoena, or other legal order. By closing this loophole, the bill prevents government agencies from conducting an end-run around the protections of the Fourth Amendment.

Background and Need for the Legislation

A. BACKGROUND

i. History and Overview of the Foreign Intelligence Surveillance Act

In 1978, Congress enacted FISA in response to revelations that the federal government had seriously abused warrantless surveillance, resulting in rampant privacy violations.[1] FISA provides a statutory framework for government agencies to conduct surveillance for foreign intelligence purposes through electronic surveillance, physical searches, pen registers and trap and trace devices, or the production of certain business records.[2] FISA also established the FISC to provide judicial oversight of government applications to conduct electronic surveillance, physical searches, and other forms of investigative actions for foreign intelligence purposes.[3]

Subsequent legislation expanded federal statutes involving foreign intelligence gathering. After the September 11, 2001, terrorist attacks, Congress enacted the USA PATRIOT Act to "provid[e] enhanced legislative tools" to "assist in the prevention of future terrorist activities and the preliminary acts and crimes which further such activities."[4] The Patriot Act and, later, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA),[5] further amended FISA.

---

[1] S. Rep. No. 94-755 (1976) (Book II, Intelligence Activities and the Rights of Americans).
[2] *See The Foreign Intelligence Surveillance Act of 1978*, Bureau of Justice Assistance U.S. Department of Justice, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286#:~:text=FISA%20was%20initially%20enacted%20in,collection%20of%20foreign%20intelligence%20information (last visited Apr. 12, 2023).
[3] *See id.*
[4] H.R. REP. NO. 107-236, at 41 (2001).
[5] Pub. L. No. 108-458 (2004).

Specifically, section 206 of the Patriot Act permitted roving wiretaps[6] and Section 6001(a) of IRTPA permitted the targeting of non-U.S. persons who are shown to be engaged in international terrorism without requiring evidence connecting those persons to a foreign power or terrorist group (lone-wolf provision).[7]

Section 215 of the Patriot Act enlarged the scope of FISA's business records provision so that the government could request "any tangible thing" about a U.S. person based on a showing that "there are reasonable grounds to believe" that those records are "relevant" to an "authorized investigation" into "international terrorist or clandestine intelligence activities."[8] This section also authorized the bulk collection of telephone metadata. In 2015, however, Congress passed the USA FREEDOM Act to reform intelligence gathering programs in the wake of Edward Snowden's disclosures.[9] The Act prohibited the bulk collection of records under Section 215 of the Patriot Act, thus narrowing Section 215's FISA authorities.[10]

In 2008, Congress enacted FISA Section 702, which allows the government to acquire foreign intelligence by targeting non-U.S. persons who are reasonably believed to be outside of the United States, for the purpose of obtaining foreign intelligence information.[11] More details about Section 702 are below.

In 2018, Congress enacted the FISA Amendments Reauthorization Act of 2017 into law, which extended Section 702 through December 31, 2023.[12] The bill required the FBI to seek a warrant when conducting queries during the "predicative" stage of an investigation but allowed the warrantless queries under Section 702 to continue in other situations.[13] Prior to 2018, Congress last reauthorized Section 702 in 2012.[14]

In 2020, Section 215 of the Patriot Act, along with the lone wolf provision and the roving wiretap provision, expired.[15] However, some of the provisions remained in effect due to a sunset clause that authorized the continued effect of the amendments regarding investigations that started, or potential offenses that took place, prior to the provisions' sunset date.[16]

---

[6] *See* Pub. L. No. 107-56 (2001).
[7] Pub. L. No. 108-458 (2004).
[8] *See* Pub. L. No. 107-56 (2001).
[9] Pub. L. No. 114-23 (2015).
[10] *See H.R. 2048, the USA Freedom Act*, H. Comm. on the Judiciary, available at https://judiciary.house.gov/usa-freedom-act (last visited Dec. 3, 2023).
[11] 50 U.S.C. § 1881a(a), (b)(3).
[12] Pub. L. No. 115-118, 132 Stat. 3 (2018).
[13] *See* Martin Matishak and Cory Bennett, *Surveillance bill heads to Trump's desk*, Politico (Jan. 18, 2018), https://www.politico.com/story/2018/01/18/fisa-bill-senate-pass-trump-293130. The "predicative" stage is the last stage before the FBI begins a formal investigation. Prior to this stage, the FBI can query communications without seeking a warrant as they build cases in non-security matters.
[14] P.L. 112-238 (Dec. 2012).
[15] *See* India McKinney, *Section 215 Expired: Year in Review 2020*, Electronic Frontier Foundation (Dec. 29, 2020), https://www.eff.org/deeplinks/2020/12/section-215-expired-year-review-2020.
[16] *Id.*

a. FISA Title I

Title I of FISA established the procedures for the government to conduct foreign intelligence surveillance and established the FISC.[17] Under Title I, the government may apply to the FISC for an order authorizing the government to conduct electronic surveillance against a particular target.[18] In applying for an order, the government must demonstrate probable cause to believe that the target is a foreign power or an agent of a foreign power.[19]

The FISC sits in Washington, D.C., and is composed of 11 district court judges selected by the Chief Justice of the United States from at least seven of the judicial circuits, and three of the judges must reside within 20 miles of the District of Columbia.[20] Typically, judges sit on the court for one week at a time on a rotational basis.[21] The presiding judge of the FISC is selected by the Chief Justice.[22] These judges are eligible to serve one term of seven years.[23]

The FISC is tasked with authorizing the government's surveillance applications.[24] Proceedings before the court are generally *ex parte*, meaning only the government is represented. In 2015, Congress amended FISA to authorize the FISC to appoint five amici curiae to assist with review of applications or to interpret the law or provide guidance on novel issues.[25] In his review of the FISA program, Department of Justice Inspector General Michael Horowitz highlighted the concerns many have with the FISC:

> FISC proceedings are ex parte, meaning that unlike most court proceedings, the government is present but the government's counterparty is not, and FISA orders generally are not subject to scrutiny through subsequent adversarial proceedings. As a result, the FBI and [DOJ's National Security Division] FISA application process is critical to ensuring that DOJ officials asked to authorize FISA applications, and judges on the FISC asked to approve them, have a complete and accurate set of facts in the FISA application on which they can rely.[26]

---

[17] *The Foreign Intelligence Surveillance Act of 1978 (FISC)*, Bureau of Justice Assistance Department of Justice, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286 (last visited Apr. 15, 2023).
[18] 50 U.S.C. § 1804.
[19] *Id.* at § 1805.
[20] Andrew Nolan and Richard M. Thompson II, *Reform of the Foreign Intelligence Surveillance Courts: Procedural and Operational Changes* at 3, CONG. RESEARCH SERVICE, (Aug. 26, 2014).
[21] *Id*.
[22] *Id*.
[23] United States Foreign Intelligence Surveillance Court, *About the Foreign Intelligence Surveillance Court* (last visited May 30, 2021).
[24] *Id.*
[25] 50 U.S.C. § 1803(i)(2).
[26] U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GEN., AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S EXECUTION OF ITS WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS at i (2021).

Because of the secretive nature of FISC proceedings, it is vital that the intelligence community comply with its own procedures for surveillance and provide the FISC with all necessary information needed to issue orders. However, as evidenced by Inspector General Horowitz's investigation and audit of the FBI's use of its FISA authorities, as well as Special Counsel John Durham's investigation of the FBI's surveillance of Carter Page, it is clear that the FBI has failed to consistently comply with these procedures and that the FISC is in need of reform.

b. FISA Section 702

Congress enacted Section 702 of FISA in 2008 as part of the FISA Amendments Act.[27] Section 702 provides an alternative to the surveillance requirements of Title I of FISA. Title VII of FISA (which includes Section 702) generally addresses electronic surveillance directed at targets outside the United States.[28] Section 702 may only be used to target:

(1) non-U.S. persons;
(2) who are reasonably believed to be outside of the United States;
(3) for the purpose of obtaining foreign intelligence information.[29]

The statute only permits the acquisition of information "from or with the assistance of an electronic communications service provider."[30] The FISC supervises such surveillance by approving certifications submitted jointly by the Attorney General and the Director of National Intelligence (DNI), ensuring that the surveillance complies with the statutory requirements of Section 702.[31] The certification must detail the targeting procedures, minimization procedures, and querying procedures that the government intends to use in its surveillance.[32] But unlike orders under Title I of FISA, the statute does not require the FISC to make probable cause determinations as to individual surveillance targets.[33] Rather, the court reviews and certifies the Attorney General and DNI's targeting procedures to ensure they are properly limited, with such authorizations effective for one year.[34]

[27] Pub. L. 110-261 (2008).
[28] *See* EDWARD C. LIU, CONG. RESEARCH SERV., R47477, REAUTHORIZATION OF TITLE VII OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2023).
[29] 50 U.S.C. § 1881a(a), (b)(3).
[30] *Id.* § 1881a(h)(2)(A)(vi).
[31] *Id.* § 1881a(j)(1)(A).
[32] *Id.*
[33] *Id.* § 1881a(j)(2).
[34] *Id.* § 1881a(a), (h)(1)(A).

1. Communications Collection

Once the FISC approves targeting procedures, the government has various ways to conduct surveillance and collect communications. These methods include downstream collection, upstream collection, and about collection.

In downstream collection, the government may direct a communications service provider (internet service provider, telephone provider, or email provider) to provide all communications to or from a selector, such as an email address, associated with a Section 702 target.[35] In upstream collection, the government directs its requests to telecommunications "backbone" providers, such as companies that operate internet cables.[36]

About, or abouts, collection has been the subject of controversy over the years. About collection involves the government capturing vast amounts of communications in which the selector (e.g., email address) of a target appeared somewhere in communications, even when the target is not a party to the communication.[37] A declassified FISC opinion shed light on this type of collection, noting that it resulted in the collection of "tens of thousands of wholly domestic communications each year" by the National Security Agency (NSA).[38] In 2017, the NSA announced that it was no longer performing "about" collection and in 2018 Congress amended Title VII to prohibit "about" collection unless the Attorney General and DNI notify the House and Senate Judiciary and Intelligence Committees that the NSA plans to resume such collection.[39] While the NSA is not currently performing this type of collection, it is free to resume it at any time, provided it notifies Congress.

2. Minimization Procedures

Under Section 702, the government is required to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning nonconsenting U.S. persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[40] For example, if the government collects communications discussing or mentioning a U.S. person, but it contains no foreign intelligence information, it must be deleted as soon as practicable but no later than five years from the Section 702 authorization's expiration subject to certain exceptions.[41]

---

[35] *See* Liu, *supra* note 28 at 10-11.
[36] *Id.* at 11.
[37] *Id.* (citing PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 37 (July 2, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/ba65702c-3541-4125-a67d-92a7f974fc4c/702-Report-2%20-%20Complete%20-%20Nov%2014%202022%201548.pdf).
[38] Redacted, 2011 WL 10945618, at *15 (FISA Ct. Oct. 3, 2011).
[39] *See* Liu, *supra* note 2828 at 12 (citing 50 U.S.C. § 1881a(b)(5)).
[40] *Id.* (citing 50 U.S.C. § 1801(h)).
[41] *Id.*

3. Querying Procedures

Much of the controversy surrounding Section 702 involves the government's querying of Section 702-acquired communications already in the government's possession, nearly always without first obtaining a warrant. While the government is required to minimize the sharing and retention of U.S. person information and communications, the NSA "routinely shares raw Section 702 data" with the other intelligence agencies.[42] Each of the intelligence agencies that have access to Section 702-acquired information—the FBI, CIA, National Counterterrorism Center (NCTC), and the NSA—establish procedures that govern how they may query such information.[43] While these agencies are required to establish procedures to limit the number of Americans affected, the amount of information available to the government is significant. According to the Privacy and Civil Liberties Oversight Board (PCLOB), an independent federal agency established to uphold civil liberties with respect to terrorism-related policies, "[a]part from communications acquired by mistake, U.S. persons' communications are not typically purged or eliminated from agency databases, even when they do not contain foreign intelligence information, until the data is aged off in accordance with retention limits."[44]

Members of Congress and privacy and civil liberties advocates have raised concerns about the querying of Section 702 data for Americans' communications as a "backdoor search." Critics disparage the tactic as an end-run around of the warrant requirement because "backdoor searches" purport to be carried out for foreign intelligence purposes while actually seeking information on Americans without a court order.[45] For example, the FBI is able to query information in most circumstances without a court's approval.[46] In a small subset of cases, the FBI is required to obtain an order from FISC authorizing a query of Section 702 communications if the query is unrelated to national security, known as "evidence of a crime only" queries. Yet in 2022, the FBI only ran such queries 16 times.[47] The FBI may conduct the vast majority of its queries without obtaining an order as long as the query is done to obtain foreign intelligence information or to pursue investigations related to national security.[48]

ii. Justice Department Office of Inspector General Audits of FISA

---

[42] Elizabeth Goitein, *The Year of Section 702 Reform, Part I: Backdoor Searches*, Just Security (Feb. 13, 2023), https://www.justsecurity.org/85068/the-year-of-section-702-reform-part-i-backdoor-searches/ (citing ATTORNEY GENERAL AND DIRECTOR OF NATIONAL INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (Sep. 2021)).

[43] *See* PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 8 (July 2, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/ba65702c-3541-4125-a67d-92a7f974fc4c/702-Report-2%20-%20Complete%20-%20Nov%2014%202022%201548.pdf.

[44] *See id.* at 8.

[45] *See* Goitein, *supra* note 422.

[46] *See* Liu, *supra* note 28 at 13.

[47] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT, CALENDAR YEAR 2022 at 27 (2023).

[48] *See Id*.

The Justice Department Office of Inspector General (OIG) has issued numerous reports documenting the FBI's mishandling of surveillance authorities. These reports largely focused on the FBI's misuse of Title I of FISA, whereby the government may apply to the FISC for an order authorizing the government to conduct electronic surveillance against a particular target.[49] In 2001, the FBI adopted the "Woods Procedures," following concerns raised by the FISC about inaccuracies in FISA applications.[50] The Woods Procedures mandate compiling supporting documentation for each fact in the FISA application. This FBI policy requires that a FISA application include a sub-file that contains: (1) supporting documentation for every factual assertion contained in a FISA applications, and (2) supporting documentation and the results of required database searches and other verifications.[51]

In December 2019, the OIG issued a 478-page report finding that the FBI had abused its FISA authority to illegally surveil former Trump campaign associate Carter Page.[52] The report found 17 significant "errors or omissions" and 51 wrong or unsupported factual assertions in the applications to surveil Page.[53] The OIG also found that the FBI downplayed the significance of the Democratic National Committee-financed opposition research document prepared by Christopher Steele (the "Steele Dossier") in the applications.[54] Per the report, the FBI cherry-picked facts to support its application, ignored exculpatory evidence, and fabricated evidence presented to a FISC judge to support its surveillance against Page.[55] This led the Justice Department to later admit that "there was insufficient predication to establish probable cause to believe that [Carter] Page was acting as an agent of a foreign power."[56]

During the 116th Congress, on February 5, 2020, FBI Director Christopher Wray testified before the House Committee on the Judiciary. During the hearing, Director Wray indicated that the FBI was taking the FISA abuses seriously and working to address them.[57] At the hearing, Director Wray testified that Americans should not "lose any sleep over" the "vast majority" of FISA applications.[58] This followed testimony from former FBI Director James Comey during a

---

[49] 50 U.S.C. § 1804.
[50] *See* 2021 DOJ OIG Audit, *supra* note 26 at i.
[51] *See* U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GEN., MANAGEMENT ADVISORY MEMORANDUM FOR DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION REGARDING THE EXECUTION OF WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS at 3 (Mar. 30, 2020).
[52] U.S. DEP'T. OF JUSTICE, OFFICE OF INSPECTOR GEN., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION (2019).
[53] *Id.* at viii & xiii
[54] *Id.* at vi.
[55] *Id.* at xi.
[56] *In re Carter W. Page*, Nos. 16-1182, 17-52, 17-375, 17-679 (FISC Jan. 7, 2020).
[57] *Oversight of the Federal Bureau of Investigation, hearing before the H. Comm. on Judiciary,* 116th Cong. (Feb. 5, 2020).
[58] *Id*. ("And the thing I would say whenever we talk about anything with FISA, when you use phrases like 'every single time,' is that it's important for the American people to understand, for this committee to understand that the vast majority of the FISAs that we do, both the initial applications and renewals, are the kinds of

transcribed interview with the Committee in December 2018, when he heralded the FBI's FISA operations as a "labor-intensive and supervision heavy" process with an emphasis on high standards.[59] Comey labeled it a "top tier" FBI program.[60] The OIG's findings undercut the FBI's former and current leaderships' stated confidence in the FISA process.

Shortly after Director Wray's testimony, as a result of the OIG's findings in 2019, the OIG conducted further analysis of the FBI's FISA processes, releasing a management advisory in March 2020.[61] The management advisory detailed the FBI's extensive noncompliance with Woods Procedures. The OIG wrote that it "do[es] not have confidence that the FBI has executed its Woods Procedures in compliance with FBI Policy, or that the process is working as it was intended to help achieve the 'scrupulously accurate' standard for FISA applications."[62] Of the 29 surveillance applications on U.S. persons that the OIG sought to examine, the FBI was unable to even locate the Woods Files for four applications.[63] There was unsupported, uncorroborated, or inconsistent information in the Woods Files of all of the remaining 25 applications reviewed.[64] The OIG "identified an average of about 20 issues per application reviewed."[65]

In September 2021, the OIG issued a more detailed report confirming its initial finding of widespread FBI non-compliance with the Woods Procedures.[66] The OIG noted that "certain public statements from the FBI . . . in 2020 failed to recognize the significant risks posed by systemic non-compliance with the Woods Procedures, and during our audit some FBI field personnel minimized the significance of Woods Procedures non-compliance."[67] In conducting an accuracy review of the 29 FISA applications, the OIG found over 400 instances of non-compliance with the Woods Procedures.[68] Of the more than 7,000 FISA applications from

---

applications that I am quite confidence – we don't know each other, but I'm quite confident you wouldn't lose any sleep over. And we really wouldn't want to grind things to a halt on that front.").

[59] James Comey Transcribed Interview 145 (Dec. 17, 2018) ("And if you know the FISA process, you know how high the standards are."); *id*. at 147 ("It's one of the things that is the most labor-intensive and supervision heavy that the FBI does. There are some things I can think of that are also very, very carefully scrubbed, but it's one of that top tier.").

[60] *Id*.. The OIG previously found that Comey made one "unauthorized disclosure of sensitive investigative information" involving President Trump, specifically in the hopes of "achiev[ing] a personally desired outcome"—the appointment of Special Counsel Robert Mueller.

[61] *See* U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GEN., MANAGEMENT ADVISORY MEMORANDUM FOR DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION REGARDING THE EXECUTION OF WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS at 3 (Mar. 30, 2020).

[62] *Id*. at 8.

[63] *Id.* at 7.

[64] *Id.*

[65] *Id.*

[66] U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GEN., AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S EXECUTION OF ITS WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS (2021).

[67] *Id.* at ii.

[68] *Id.* at 7.

January 2015 through March 2020, there were 179 instances of missing, destroyed, or incomplete Woods Files, in addition to the four discovered in the March 2020 review.[69]

iii. Special Counsel John Durham Report

On May 12, 2023, Special Counsel John Durham issued his report investigating the intelligence activities and investigations arising out of the 2016 presidential campaigns, namely, the FBI's Crossfire Hurricane investigation. As did the OIG, Special Counsel Durham reviewed the FBI's use of its FISA authorities to surveil Carter Page. And, like the OIG, the Special Counsel's report identified significant abuses of the FBI's FISA authorities.

The Special Counsel's report found that the FBI's FISA applications to surveil Trump campaign associate Carter Page were based almost entirely on the debunked allegations in the Steele dossier.[70] The information relied largely on subsources, none of whom the FBI interviewed could corroborate any of the information in the Steele dossier.[71] For example, the FBI never interviewed Charles Dolan, likely the source of several of the allegations.[72] Despite the lack of evidence, two days after receiving Steele dossier information, the FBI incorporated the information into its Page FISA application.[73] Some FBI agents even expressed concern over the reliability of the information but were pressured by FBI leadership to open a full investigation.[74] As it pressed forward with the investigation, the FBI used confidential human sources to obtain more information, but mischaracterized and misstated intelligence gathered by the sources, errors that were included in all three renewal FISA applications.[75] Ultimately, Carter Page was subjected to illegal surveillance for eleven months.[76]

iv. Abuses of FISA Section 702

While the Justice Department OIG and Special Counsel Durham have thoroughly detailed abuses and deficiencies in FISA Title I applications, there are separate, significant concerns related to Section 702, particularly with querying procedures. Despite the statute's limitation of surveillance to foreign nationals, "Section 702 has become a rich source of warrantless government access to Americans' phone calls, texts, and emails."[77] That is because

---

[69] *Id.*
[70] Office of Special Counsel John H. Durham, *Report on Matters Related to Intelligence Activities and Investigations Arising out of the 2016 Presidential Campaigns*, U.S. Dep't of Justice at 117, 134 [hereinafter: "Special Counsel's Report"].
[71] *Id.* at 228.
[72] *Id.* at 172.
[73] *Id.* at 117.
[74] *Id.* at 102.
[75] *Id.* at 208-09, 212.
[76] U.S. DEP'T. OF JUSTICE, OFFICE OF INSPECTOR GEN., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION at vi (2019).
[77] *Section 702 of FISA: A "Foreign Intelligence" Law Turned Domestic Spying Tool*, The Brennan Center for Justice (Feb. 2, 2023), https://www.brennancenter.org/our-work/research-reports/coalition-document-proposes-reforms-section-702.

rather than minimizing the sharing and retention of Americans' data, "the NSA routinely shares such data with the FBI, CIA, and National Counterterrorism Center, and all agencies retain it for at least five years."[78] While the government may not intentionally acquire communications from senders or recipients that are located in the United States,[79] it frequently "incidentally" acquires this information.[80] Section 702 permits the government to target foreigners abroad in search of "foreign intelligence information," which is interpreted broadly and often has no nexus to national security.[81]

In 2014, the Privacy and Civil Liberties Oversight Board (PCLOB) issued a comprehensive unclassified report of the Section 702 program.[82] The 2014 report issued 12 recommendations and noted the privacy risks inherent in this surveillance program due to the large scope of "incidental" collection of U.S. persons communications, the use of "about" collection, and the use of queries to search the communications of specific U.S. persons.[83]

The FBI, NSA, CIA, and NCTC are all authorized to query Section 702-acquired content for foreign intelligence information.[84] But only the FBI is authorized to conduct queries that are reasonably likely to return evidence of a crime.[85] Because of this, the FBI conducts U.S. person queries at a higher rate than other intelligence agencies.[86] In January 2023, the PCLOB hosted a public forum to discuss the potential reauthorization of FISA Section 702 and highlight issues with the program and the need for reform.[87] In her testimony at this forum, Cindy Cohn, Executive Director of the Electronic Frontier Foundation, noted that one of the major concerns with Section 702 is the fact that the "fruits of this surveillance don't just stay with the NSA . . . [they] stretch over to the FBI which means they are available for prosecution and indeed have been used for prosecution."[88] These use cases raise questions about whether a tool designed for foreign intelligence gathering has been transformed into a weapon for the FBI to use in its domestic law enforcement mission capacity.

---

[78] *Id.*
[79] 50 U.S.C. § 1881a(b).
[80] *See Warrantless Surveillance Under Section 702 of FISA*, ACLU, https://www.aclu.org/issues/national-security/privacy-and-surveillance/warrantless-surveillance-under-section-702-fisa (last visited Apr. 17, 2023).
[81] *Id.*
[82] *See* PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014).
[83] *Id.* at 93, 111, 123, 134.
[84] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT, CALENDAR YEAR 2021 at 19 (2022).
[85] *Id.*
[86] *Id.* at 20.
[87] U.S. Privacy and Civil Liberties Oversight Board, *PCLOB Public Forum on FISA Section 702*, YOUTUBE (Jan. 12, 2023), https://www.youtube.com/watch?v=AZvaimMTqio.
[88] *Id.* at min. 1:34:50.

In October 2023, the PCLOB issued a new report, calling for various legislative and internal changes to the Section 702 program.[89] While stating that "Section 702 remains highly valuable to protect national security," the PCLOB also found that the program "creates serious privacy and civil liberties risks."[90] To address these issues, the PCLOB made 19 legislative and administrative recommendations, most notably a requirement that the FISC review and authorize U.S. person queries.[91] Other recommendations include a prohibition on "abouts" collection, further reporting and transparency measures, additional audits of the Section 702 program, and more robust amici authority in the FISC.[92]

a. Constitutional Concerns with Warrantless Searches

The FBI's use of Section 702 certainly implicates the privacy and civil liberties of Americans, but it also may violate the Fourth Amendment to the Constitution. The FISC has repeatedly held that queries of Section 702-acquired information do not violate the Fourth Amendment, stating that the "targeting, minimization, and querying procedures, as written, are consistent with the requirements of the Fourth Amendment" and "adequately guard against error and abuse."[93]

The FISC's view of the constitutionality of such searches has been challenged in the past, however. Following the enactment of new querying provisions in the FISA Amendments Reauthorization Act of 2017, amici argued that the FISC "should regard queries as distinct Fourth Amendment searches."[94] The FISC declined to do so, stating that although Congress believed that "Fourth Amendment concerns are implicated by Section 702 queries," the FISC determined that the law expanded statutory protections, but not the scope of what constitutes an unlawful search under the Fourth Amendment.[95]

In contrast, in 2019, the U.S. Court of Appeals for the Second Circuit held that Section 702 queries do implicate the Fourth Amendment and found that each query should be regarded as "a separate Fourth Amendment event that, in itself, must be reasonable."[96] The Court raised concerns about the ability to query such a vast trove of communications, stating that permitting:

> that information to be accessed indiscriminately, for domestic law enforcement purposes, without any reason to believe that the individual is involved in any criminal activity and or even that any

[89] *See* PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2023).
[90] *Id.* at 7.
[91] *Id.* at 205-08.
[92] *See generally id.* at 208-25.
[93] *See* Memorandum Opinion and Order, *Document re: Section 702 2021 Certification* at 66 (FISA Ct. Apr. 21, 2022).
[94] *Id.* at 63.
[95] *Id.* (citing Memorandum Opinion and Order at 87 (FISA Ct. Oct. 18, 2018)).
[96] *United States v. Hasbajrami*, 945 F.3d 641, 672 (2d Cir. 2019).

> information about the person is likely to be in the database, just to see if there is anything incriminating in any conversations that might happen to be there, would be at odds with the bedrock Fourth Amendment concept that law enforcement agents may not invade the privacy of individuals without some objective reason to believe that evidence of crime will be found by a search.[97]

The Second Circuit's decision takes into account technological changes and the vast amount of information that is collected under Section 702 and raises questions about whether such "backdoor searches" are constitutional.[98] The court explained that "[t]hat concern is compounded by the hundreds of thousands of searches done by the government's aggregate querying of Section 702, representing a massive violation of Americans' privacy."[99] Although the FISC disagreed with the Second Circuit in its 2022 opinion, the FBI's continued violations of its Section 702 authorities raise concerns that it is violating the Fourth Amendment. As Congress considers reforms to Section 702, it cannot rely on the FBI to enact internal changes and police itself. Despite claims of change and improvement, the FBI has consistently violated its Section 702 authorities and Congress must act to protect the constitutional rights of Americans.

b. ODNI Annual Statistical Transparency Report

According to the Office of the Director for National Intelligence (ODNI), the FBI has misused FISA-collected information to surveil Americans without a warrant.[100] In 2021, ODNI data revealed that the FBI conducted an estimated 3,394,053 U.S. person queries[101] and in 2022 the FBI conducted 204,090 searches, or roughly 559 per day.[102]

In its 2022 annual statistical transparency report, ODNI noted that the FBI updated its counting methodology to allow it to identify the number of unique U.S. person query terms, rather than just the total number of queries, as it had done in the past.[103] This methodology eliminates duplicate queries and is more in line with the methods of other intelligence community elements.[104] Based on the "de-duplicated" counting methodology, the FBI reports that it conducted 119,383 U.S. person queries in 2022 compared to a de-duplicated number of 2,964,643 in 2021 (as opposed to 204,090 queries and 3,394,053 queries, respectively).[105] Even

---

[97] *Id.* at 672.
[98] *See* Andrew Crocker, *The Foreign Intelligence Surveillance Court Has Made a Mockery of the Constitutional Right to Privacy*, Electronic Frontier Foundation (June 1, 2023), https://www.eff.org/deeplinks/2023/06/foreign-intelligence-surveillance-court-has-made-mockery-constitutional-right.
[99] *Id.*
[100] *See generally* 2021 ODNI Annual Statistical Transparency Report, *supra* note 844.
[101] *Id.* at 4, 21.
[102] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT, CALENDAR YEAR 2022 at 24 (2023).
[103] *Id.* at 23.
[104] *Id.*
[105] *Id.* at 24.

with an updated counting methodology, such a precipitous drop – over 95% lower – does raise questions as to the efficacy of the program and should garner scrutiny to ensure the method is being applied with integrity. And though this counting method is consistent with those used by the CIA, NSA, and NCTC, it is not perfect. For example, when the FBI uses a U.S. person identifier to query unminimized Section 702-acquired information, that will now be counted as a single query term, regardless how many times the FBI uses that term.[106]

In recent years, Congress and the FISC have sought to impose limits on these backdoor searches. Those proposals include requiring the FBI to show probable cause and obtain an order from the FISC for queries in "predicated criminal investigations that do[] not relate to the national security of the United States."[107] However, because the FBI often runs queries before an investigation is predicated, this requirement is rarely triggered.[108] Even when such a requirement is triggered, as it has been approximately 100 times since 2018, the FBI rarely complies.[109] For the vast majority of cases, the only limitation is the requirement that U.S. person queries must be reasonably likely to return foreign intelligence or evidence of a crime—a low bar.[110]

c. ODNI Semiannual Report

Analysis of Section 702 in recent years reveals the extent of the problem of this type of warrantless surveillance. The Justice Department and ODNI released an unclassified copy of their 24th semiannual assessment of FISA Section 702 in December 2022.[111] The report details issues ranging from conducting queries unlikely to return foreign intelligence information, evidence of ordinary criminal activity, and conducting overly broad queries. Recently, Congressman Darin Lahood (R-IL) revealed that he was likely subjected to wrongful FISA queries multiple times.[112] The semiannual report determined this search was improper, as the FBI conducted a query using only the Congressman's name, with no limiters, potentially returning troves of sensitive communications.[113]

Additionally, the FBI is also using Section 702 to search the communications of everyday Americans. The 24th semiannual report also uncovered information about the FBI's queries of individuals who had requested to participate in the FBI's "Citizens Academy," individuals who came to an FBI field office to conduct repairs, and individuals who entered a field office to

---

[106] *Id.* at 25.
[107] *See* 50 U.S.C. § 1881a(f)(2); *see also* Goitein, *supra* note 422.
[108] *See* Goitein, *supra* note 422.
[109] *Id.* (citing OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT, CALENDAR YEAR 2021 at 19 (2022)).
[110] *Id.*
[111] DEPARTMENT OF JUSTICE AND OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (December 2021). This report covers the timeframe of December 1, 2019 through May 31, 2020.
[112] *See* Charlie Savage, *Lawmaker Says He Was Target of F.B.I. Surveillance Material Searches*, THE NEW YORK TIMES (March 9, 2023).
[113] *See* 24th DOJ-ODNI Semiannual Assessment, *supra* note 111 at 58 fn. 92.

provide a tip or to report that they were the victim of a crime.[114] The FBI also queried the names of a local political party to determine if it had any connections to foreign intelligence; the report found that this query "was not reasonably likely to achieve foreign intelligence information."[115] The FBI has also searched for the communications of journalists, college students participating in a "Collegiate Academy," police officer candidates, and colleagues and relatives of the FBI agent performing the search, among others.[116]

In 2023, the Justice Department and ODNI released unclassified copies of their 25th and 26th semiannual assessments, covering June 1, 2020, through November 30, 2020, and December 1, 2020, through May 31, 2021, respectively. While the number of querying incidents declined from the previous reporting periods, the reports still showed querying violations. For example, the 25th semiannual assessment identified querying violations as a result of FBI personnel conducting overly broad queries, queries unlikely to return foreign intelligence information, or being unaware that a query would be run against FISA-acquired information.[117] FBI personnel also conducted U.S. person queries to research prospective law enforcement personnel.[118] Similarly, while the 26th semiannual assessment showed a decrease in querying compliance incidents, FBI personnel violated the querying standards on various occasions, such as by failing to properly document the justification for a query or improperly conducting batch queries.[119]

d. FISC Opinions

On May 19, 2023, the ODNI released two unclassified FISC opinions, including the 2021 FISA Section 702 Certifications and Targeting, Minimization, and Querying Procedures opinion, initially issued in April 2022.[120] This opinion included results from the Justice Department's National Security Division (NSD) audit and the FBI's Office of Internal Auditing audit of query compliance generally between 2020 and 2021. While the Justice Department and FBI have continually told Congress and the FISC that it is making changes to its querying procedures, the FISC opinion demonstrates continued querying violations.

For example, according to the opinion, FBI agents ran a batch query of unminimized FISA information in June 2020, using identifiers of over 100 individuals in connections with the

---

[114] *Id.* at 58.
[115] *Id.*
[116] *See Section 702 of FISA: A "Foreign Intelligence" Law Turned Domestic Spying Tool*, The Brennan Center for Justice (Feb. 2, 2023), https://www.brennancenter.org/our-work/research-reports/coalition-document-proposes-reforms-section-702.
[117] DEPARTMENT OF JUSTICE AND OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT at 55-56 (April 2022).
[118] *Id.* at 56.
[119] DEPARTMENT OF JUSTICE AND OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT at 55-57 (August 2022).
[120] *See* Memorandum Opinion and Order, *Document re: Section 702 2021 Certification* (FISA Ct. Apr. 21, 2022).

George Floyd protests without "any specific potential connections to terrorist related activity" known to the FBI.[121] The Justice Department's NSD assessed that those searches were unlikely to return foreign intelligence information or evidence of a crime.[122] Additionally, multiple FBI agents ran queries against unminimized information of individuals suspected of involvement in the events that occurred at the Capitol on January 6, 2021.[123] This included a query of "thousands of names within FBI systems in relation to the Capitol breach investigation," including running thirteen names against unminimized data in order to determine if any individuals had foreign ties.[124] Another agent conducted 360 queries in connection with drug investigations, domestic terrorism investigations, and January 6, 2021, without providing any information to support a reasonable belief that the query would return foreign intelligence information or evidence of a crime.[125]

Reports also revealed the FBI conducted a batch query for over 19,000 donors to a congressional campaign in an attempt to determine if it was a target of foreign influence, and the NSD determined that only eight of the identifiers used had a sufficient connection to foreign influence activities to justify such a search.[126] In total, the FBI conducted more than 278,000 improper searches of U.S. persons' communications, including information acquired pursuant to Section 702.[127]

Despite the FBI's claims that its internal remedial measures have resulted in increased compliance, the FISC's 2023 FISA Section 702 Certifications and Targeting, Minimization, and Querying Procedures opinion identified further violations. For example, the FBI conducted various queries without receiving Deputy Director approval before using a "sensitive query term," a violation of the FBI's recently-adopted procedures.[128] In June 2022, an analyst conducted four queries of Section 702 information using the last names of a United States Senator and a state senator based on information that a foreign intelligence service was targeting those individuals.[129] The analyst not only failed to receive requisite approval, but the NSD also determined the querying standard of "reasonably likely to retrieve" foreign intelligence information was not met.[130] Another agent ran a query using the social security number of a state judge who "had complained to the FBI."[131]

e. Use of Section 702 in Court

---

[121] *Id.* at 27 (internal quotations omitted).
[122] *Id.*
[123] *Id.* at 28.
[124] *Id.*
[125] *Id.* at 29.
[126] *Id.*
[127] *Id.* at 31.
[128] *See* Memorandum Opinion and Order, *Document re: Section 702 2023 Certification* at 86 (FISA Ct. Jul. 21, 2023).
[129] *Id.*
[130] *Id.*
[131] *Id.*

A significant concern arises when Section 702-acquired information is used against a defendant in court.[132] While the law generally requires the government to notify defendants when information "derived from" FISA Section 702 electronic surveillance is used to investigate them,[133] there are several loopholes the government exploits to avoid this requirement.[134] For example, the Justice Department reportedly relies on a "secret interpretation" of the phrase "derived from," leading it often to determine no notification is required.[135] The government also uses "parallel construction" whereby "government officials are alerted to illegal activity, but instead of divulging the fact that they received this information from a secret database, they tip off local officials" allowing them to discover information from a different source.[136]

In a 2020 opinion, the FISC sounded the alarm about the FBI's actions in using FISA-acquired data for domestic criminal and other non-intelligence purposes. The court noted the discovery of 40 queries in which the FBI accessed information for investigations involving "health-care fraud, transnational organized crime, violent gangs, domestic terrorism involving racially motivated violent extremists, as well as investigations relating to public corruption and bribery," none of which were "related to national security, and they returned numerous Section 702-acquired products in response."[137]

f. The Need for a Warrant Requirement

Such consistent violations of FISA demonstrate the need to include a warrant requirement for U.S. person queries in any reauthorization of the Act. On July 14, 2023, the Subcommittee on Crime and Federal Government Surveillance of the Committee on the Judiciary held its second hearing of the 118th Congress on the need to reform FISA.[138] There, each witness highlighted the merits of such a warrant requirement.[139] According to one witness, Professor Jonathan Turley, the warrantless searches that have so often occurred under Section 702 "threaten a host of rights including free speech, the free press, freedom of religion, and free association."[140]

Additionally, Elizabeth Goitein, Senior Director of the Liberty and National Security Program at the Brennan Center for Justice at NYU School of Law, testified that "[w]arrantless access to Americans' communications has become a core feature of a surveillance program that

---

[132] *See* Jake Laperruque, *CDT Issue Brief: FISA Section 702 Key Reforms*, Center for Democracy & Technology (Jan. 30, 2023), https://cdt.org/insights/cdt-issue-brief-fisa-section-702-key-reforms/.
[133] 50 U.S.C. § 1806(c), (d).
[134] *See* Laperruque, *supra* note 1322.
[135] *Id.*
[136] *How Rand Paul plans to overhaul FISA surveillance program*, FOXBusiness (Jan. 10, 2018), https://www.foxbusiness.com/politics/how-rand-paul-plans-to-overhaul-fisa-surveillance-program.
[137] Memorandum Opinion and Order, *Document re Section 702 Certification* at 42 (FISA Ct. Nov. 18, 2020).
[138] *Fixing FISA, Part II, Hearing Before the Subcomm. on Crime and Fed. Gov't Surveillance*, 117th Cong. (2023).
[139] *Id.*
[140] *Id.* (Testimony of Professor Jonathan Turley at 1).

purports to be solely foreign-focused."[141] Goitein noted that government officials have defended these back door searches as merely searches of lawfully acquired information, so the agencies "may use the information for any government purpose."[142] In countering this argument, she highlighted that, in the law enforcement context outside of FISA, a warrant is normally required to search the contents of communications and the Supreme Court has held that officers must obtain a warrant to search cell phone data even when the cell phone was lawfully seized without a warrant incident to arrest.[143]

Goitein's testimony demonstrated that it logically follows that the search of communications acquired under FISA Section 702 should be subject to those same limitations, stating that "[t]he starting point for any reauthorization of Section 702 must be an end to warrantless searches of Americans' 'incidentally' obtained communications."[144] In the same hearing, attorney Gene Schaerr similarly stated that as a condition to reauthorizing Section 702, Congress should require that "government access to Americans' communications or other private data be allowed *only* pursuant to a judicial order, issued under the Fourth Amendment probable cause standard."[145] Such a requirement would "prevent the government from invading Americans' privacy when there is no good reason to do so."[146]

While opponents of a warrant requirement often state that requiring a warrant would prevent the intelligence officials from protecting victims, cybersecurity and civil liberties experts have consistently supported a warrant requirement, noting that such a requirement "is not just feasible, it is also essential to preventing misconduct."[147] Some of the worst surveillance abuses were conducted under the guise of protecting victims, such as the surveillance of Martin Luther King and the recent querying violation of Congressman LaHood.[148] A warrant requirement can coexist with the need to protect victims by, for example, allowing the intelligence community to conduct searches with the consent of the victim.[149] A warrant requirement will help to prevent misconduct by the intelligence community and ensure that the government only conducts a search when it has probable cause "to believe that any harm is being or is about to be inflicted on the Nation or one of its citizens."[150]

---

[141] *Id.* (Testimony of Elizabeth Goitein at 9).
[142] *Id.*
[143] *Id.* (Testimony of Elizabeth Goitein at 10 n. 48) (citing *Riley v. California*, 573 U.S. 373 (2014)); *see also id.* at n. 48 (quoting *United States v. Odoni*, 782 F.3d 1226, 1237-38 (11th Cir. 2015) ("We . . . must analyze the search and the seizure separately, keeping in mind that the fact that police have lawfully come into possession of an item does not necessarily mean they are entitled to search that item without a warrant.")).
[144] *Id.* (Testimony of Elizabeth Goitein at 23).
[145] *Id.* (Testimony of Gene Schaerr at 2).
[146] *Id.* (Testimony of Gene Schaerr at 3).
[147] Jake Lapperuque and Greg Nojeim, *CDT FISA Issue Brief: A Warrant Rule for US Person Queries Would Not Prevent Victim-Focused Queries*, Center for Democracy & Technology (Oct. 17, 2023), https://cdt.org/insights/cdt-fisa-issue-brief-a-warrant-rule-for-us-person-queries-would-not-prevent-victim-focused-queries/.
[148] *Id.*
[149] *Id.*
[150] *Fixing FISA, Part II, Hearing Before the Subcomm. on Crime and Fed. Gov't Surveillance*, 117th Cong. (2023) (Testimony of Gene Schaerr at 3).

g. The Executive Branch's Push for a Clean Reauthorization of Section 702

Despite the clear evidence of abuse, the intelligence community is pushing for a clean reauthorization of Section 702. At the PCLOB public forum in January 2023, General Paul M. Nakasone of U.S. Cyber Command gave the keynote address, urging the reauthorization of FISA Section 702. In this address, he described Section 702 as "one of the most important intelligence legal authorities for addressing U.S. threats" and called the Act "irreplaceable."[151] General Nakasone described Section 702 as an "agile" and "technology-neutral" legal authority in the fight against cybersecurity attacks.[152] He dismissed concerns over privacy violations by citing preventative measures already in place to protect civil liberties, including through annual training, policy controls on when and how queries are performed, technical controls on access to the data, the self-reporting by agencies, and oversight by all three branches of government.[153]

On February 28, 2023, President Biden's National Security Advisor Jake Sullivan similarly issued a statement calling Section 702 "a cornerstone of U.S. national security," an "invaluable tool that continues to protect Americans every day," and called its reauthorization a "top priority for the Administration."[154] That same day, Attorney General Merrick Garland and Director of National Intelligence Avril Haines sent a letter to congressional leadership urging the reauthorization of Section 702.[155]

On March 1, 2023, Attorney General Garland testified before the United States Senate Committee on the Judiciary, expressing support for the reauthorization of Section 702, noting that the Act "is subject to robust targeting, minimization, and querying procedures to protect the privacy and civil liberties of U.S. persons."[156] On July 12, 2023, FBI Director Christopher Wray testified before the House Committee on the Judiciary, similarly expressing support for Section 702.[157] Specifically, Director Wray expressed concerns about the proposal that the FBI obtain a

---

[151] U.S. Privacy and Civil Liberties Oversight Board, *PCLOB Public Forum on FISA Section 702*, YOUTUBE at min. 8:30 (Jan. 12, 2023), https://www.youtube.com/watch?v=AZvaimMTqio.
[152] *Id.* at min. 11:30.
[153] *Id.* at min. 17:13
[154] *Statement by National Security Advisor Jake Sullivan on the Biden-Harris Administration's Support for the Reauthorization of Vital Intelligence Collection Authorities*, The White House (Feb. 28, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/02/28/statement-by-national-security-advisor-jake-sullivan-on-the-biden-harris-administrations-support-for-the-reauthorization-of-vital-intelligence-collection-authorities/.
[155] *See* Letter from Merrick Garland, Attorney General, and Avril Haines, Dir. of Nat. Intelligence, to Charles Schumer, Majority Leader, U.S. Senate, Kevin McCarthy, Speaker, U.S. House of Representatives, Mitch McConnell, Minority Leader, U.S. Senate, and Hakeem Jeffries, Minority Leader, U.S. House of Representatives Minority Leader (Feb. 28, 2023), *available at* https://s3.documentcloud.org/documents/23692331/garland-haines-fisa702-letter.pdf.
[156] *See Oversight of the United States Department of Justice: Hearing Before the S. Comm. on the Judiciary,* 118th Cong. (Mar. 1, 2023) (Testimony of Hon. Merrick Garland, Att'y Gen., U.S. Dep't of Justice, at 8).
[157] *See Oversight of the Federal Bureau of Investigation: Hearing Before the H. Comm. on the Judiciary*, 118th Cong. (Jul. 12, 2023) (Testimony of Hon. Christopher Wray, Dir., Fed. Bureau of Investigation).

warrant before conducting queries of U.S. person communications, stating, "A warrant requirement would amount to a *de facto* ban, because query applications either would not meet the legal standard to win court approval" or would cause the FBI to expend vast resources and time that "in the world of rapidly evolving threats, the government often doesn't have."[158] He testified that the FBI's internal measures have improved the FBI's query compliance rate.[159]

The FBI has stated that beginning in the second half of 2021, it has made changes relating to queries of Section 702-acquired information designed to prevent the abuses of recent years.[160] Changes include requiring attorney approval for batch queries of over 100 or more queries, requiring FBI users to affirmatively opt-in to query Section 702-acquired information, updated guidance and training, and enhanced approval requirements for sensitive queries, such as those involving public officials.[161]

These statements and claims of reform ignore the clear abuse that has occurred for years. Whether the result of a misunderstanding of the querying procedures or something more nefarious, queries that involve U.S. persons should raise oversight sensitivities. For years, the FBI has claimed to have made improvements to limit the warrantless surveillance of Americans, but abuses continue to be exposed. The intelligence community, and the FBI in particular, is failing to protect the civil rights and liberties of the American people it is entrusted to protect.

v. Electronic Communications Privacy Act

Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA) to limit the government's ability to access digital communications.[162] Under ECPA, the government must seek a warrant or other court order before compelling certain electronic communications services providers to disclose the contents and records of electronic communications. These warrant and order requirements, however, only apply to certain communications services providers.

ECPA prevents a Remote Computing Service (RCS) and an Electronic Communications Service (ECS) provider from knowingly disclosing communications contents to third parties under certain circumstances. An RCS means the "provision to the public of computer storage or processing services by means of an electronic communications system."[163] An ECS means "any service which provides to users thereof the ability to send or receive wire or electronic

---

[158] *Id.* (Testimony of Hon. Christopher Wray, Dir., Fed. Bureau of Investigation at 13).
[159] *Id.*
[160] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT, CALENDAR YEAR 2022 at 23 (2023).
[161] *Id.* at 23.
[162] Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim, Dhanaraj Thakur, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, Center for Democracy & Technology at 15 (2021).
[163] 18 U.S.C. § 2711(2).

communications."[164] These include phone companies like AT&T and Verizon, and tech companies like Google, Microsoft, and Facebook.

An ECS provider is prohibited from disclosing to third parties "the contents of a communication while in electronic storage by that service,"[165] while an RCS provider cannot disclose "the contents of any communication which is carried or maintained on that service."[166] Both providers are prohibited from knowingly divulging non-content information to the government absent an exception.[167] The government may obtain subscriber information, like names, addresses, and phone numbers, from an RCS or ECS by issuing a subpoena.[168] It may obtain more sensitive non-content information like traffic or transactional information by obtaining a separate order after demonstrating "specific and articulable facts showing that there are reasonable grounds to believe" that the information is "relevant and material to an ongoing criminal investigation."[169] When the government seeks to obtain the content of electronic communications, it must obtain a probable cause warrant.[170]

However, ECPA does not restrict the ability of these electronic services providers from voluntarily providing non-content information to non-government third parties.[171] As long as those third parties are not RCS or ECS providers, then ECPA does not apply to them and does not prohibit their selling the information to the government.[172] This has led to a loophole whereby RCS and ECS providers can transfer data to private third parties and the government is able to purchase the data from those third parties without obtaining the otherwise required court order, subpoena, or warrant.

At a July 14, 2023, hearing of the Subcommittee on Crime and Federal Government Surveillance, witnesses addressed this data broker loophole.[173] One testified that "the law is woefully outdated. It does not cover digital data brokers or many app developers, for the simple reason that they did not exist in 1986, when the law was passed. This gap creates an easy end-run around the law's protections."[174] Data brokers serve as a "middleman" and allow the government to sidestep the requirements of the Fourth Amendment.[175]

vi. Supreme Court Precedent on Location Data

---

[164] 18 U.S.C. § 2510(15).
[165] 18 U.S.C. § 2702(a)(1).
[166] 18 U.S.C. § 2702(a)(2).
[167] *See* 18 U.S.C. § 2702(a)(3), (b).
[168] *See* 18 U.S.C. § 2703(c)(2).
[169] Shenkman, et al. *supra* note 162 at 16; See *also* 18 U.S.C. § 2703(d).
[170] Shenkman, et al. *supra* note 162 at 16.
[171] *Id.*
[172] *Id.*
[173] *See Fixing FISA, Part II: Hearing Before the Subcomm. On Crime and Fed. Gov't Surveillance*, 117th Cong. (2023).
[174] *Id.* (Testimony of Elizabeth Goitein at 39).
[175] *Id.*

Over 40 years ago, the Supreme Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[176] The Court has relied on this "third-party doctrine" over the years to find that the Fourth Amendment does not protect records or information voluntarily shared with someone else.[177] In 2018, in *Carpenter v. United States*, however, the Court held "that the Government must generally obtain a warrant supported by probable cause before acquiring" cell-site location information for a seven-day period.[178] Writing for the Court, Chief Justice Roberts highlighted the "seismic shifts in digital technology" that makes tracking a person's location possible.[179] The Court recognized that location information "provides an intimate window into a person's life, revealing not only his particular movements, but through them, his 'familial, political, professional, religious, and sexual associations.'"[180]

While the Court's decision in *Carpenter* dealt with cell-site location information, rather than commercially available geolocation data, "the Court's reasoning surrounding the privacy concerns of location data strongly suggest that collection of a multitude of sensitive digital information . . . is also covered by the Fourth Amendment's warrant requirement."[181] However, the government has construed *Carpenter*'s holding as limited to the facts of the case. Indeed, the Court "expressly declined to consider what other types of information might qualify for Fourth Amendment protection despite being disclosed to a third party."[182]

vii. Data Collection, Retention, and Sale

Today, data is often referred to as the world's most valuable resource, even surpassing oil.[183] It can include information from public sources, such as "demographic information, property records, court filings, criminal convictions, professional licenses, census data, birth certificates, marriage licenses, divorce records," bankruptcy records, and voter registration information, among others.[184] Commercially-sourced data may include "purchase history, warranty registration, credit information, employment registration, loyalty card data, membership data, subscriptions, etc." And still yet, even more intimate data can be procured through the collection of information originating from "social media profiles, web browsing

[176] *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (citing *United States v. Miller*, 425 U.S. 435, 442-44 (1976)).
[177] *See* Amy Howe, *Opinion analysis: Court holds that police will generally need a warrant for sustained cellphone location information*, SCOTUSblog (Jun. 22, 2018), https://www.scotusblog.com/2018/06/opinion-analysis-court-holds-that-police-will-generally-need-a-warrant-for-cellphone-location-information/.
[178] *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018).
[179] *Id.* at 2219.
[180] *Id.* at 2217 (citing *United States v. Jones*, 565 U.S. 400, 415 (Sotomayor, J., concurring)).
[181] Shenkman, et al. *supra* note 1622 at 18.
[182] *See Fixing FISA, Part II: Hearing Before the Subcomm. On Crime and Fed. Gov't Surveillance*, 117th Cong. (2023) (Testimony of Elizabeth Goitein at 41).
[183] Kiran Bhageshpur, *Data Is The New Oil – And That's A Good Thing*, FORBES (Nov. 15, 2019).
[184] Henrik Twetman, *Gundars Bergmanis-Korats, Data Brokers and Security: Risks and vulnerabilities related to commercially available data*, NATO STRATEGIC COMMC'NS CTRE. OF EXCELLENCE (Jan. 20, 2020).

activity, mobile apps, media reports, websites, mail-in rebate forms, forum posts, web browser cookies, plugins, addons, device data, IP fingerprints, network data, metadata" and so on.[185]

Data brokers aggregate, package, and sell the data acquired from a variety of sources, including those described above. Often, data brokers have thousands of different data points reflecting information about a person that, when combined, reveal valuable and intimate insights about an individual that would otherwise be unavailable.[186] In other words, for data brokers, consumers and their information are the product. For example, data brokers can receive geolocation data, sometimes accurate to just a few yards, from a mobile device up to 14,000 times per day.[187] This data allows a purchaser to identify patterns that can reveal where a person lives, where they work, and where they spend their free time.[188] This information can be useful in commercial applications, such as advertising.[189] However, it can also be exploited to learn about a person's daily life and to track their historic movements.[190]

As a result of the nature of this information, it is extremely attractive to government agencies, and recent reporting indicates that data-based policing is becoming increasingly prevalent. For example, the Internal Revenue Service (IRS), Drug Enforcement Administration (DEA), FBI, Department of Homeland Security (DHS), and Department of Defense (DOD) have all purchased geolocation information from data brokers.[191] And other experts have found that the practice of law enforcement and intelligence agencies buying sensitive data—ranging from geolocation to personal communications—is increasing, with some agencies spending "tens of millions of dollars on multi-year contracts."[192]

In recent years, the government has turned to data brokers like Venntel to purchase location data from Americans' smartphones. The IRS purchased access to a commercial database that "records the locations of millions of American cellphones" to attempt to "identify and track potential criminal suspects."[193] Another data broker, Clearview AI, developed a facial recognition software to create a database of photos from sites like Facebook, LinkedIn, and Twitter and marketed to law enforcement.[194] Because ECPA does not protect consumers from

---

[185] *Id.*
[186] *What Are Data Brokers – And What Is Your Data Worth*?, WEBFX (Mar. 16, 2020).
[187] Jennifer Valentino-DeVries, et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018).
[188] *See Id*.
[189] *Id*.
[190] *Id*.
[191] Elizabeth Goitein, *The government can't seize your digital data. Except by buying it.*, WASH. POST (Apr. 26, 2021).
[192] Sharon Bradford Franklin, Greg Nojeim & Dhanaraj Thakur, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, CTR. FOR DEMOCRACY & TECH. (Dec. 9, 2021).
[193] *See* Byron Tau, *IRS Used Cellphone Location Data to Try to Find Suspects*, WALL STREET JOURNAL (Jun. 19, 2020), https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815.
[194] *See* Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, THE NEW YORK TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

data brokers that collect their information, the government purchases data as way to avoid seeking a warrant as would otherwise be required by the Fourth Amendment.[195]

This year, the FBI admitted to buying "precise geolocation data derived from mobile-phone advertising."[196] At a hearing before the Senate Select Committee on Intelligence, Director Wray stated that the FBI now seeks court orders when obtaining phone data from commercial vendors, but the data broker loophole in ECPA would permit the FBI to resume purchasing such data in the future.[197] Leaked documents also revealed that Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) purchased cell phone location data, and ICE also purchased utility data and information from private license plate reader databases.[198] Defense contractors reportedly purchased location data from Muslim prayer apps and dating apps.[199] The Secret Service and DOD have also purchased smart phone location data.[200]

As part of the House Committee on the Judiciary's investigation into the IRS's troubling visit to the home of journalist Matt Taibbi on the day he testified before the Select Subcommittee on the Weaponization of the Federal Government, the Committee discovered that the IRS collected personal data from data brokers to use in its investigation of Taibbi.[201] For example, the IRS collected data from the data broker Anywho, a People Search Website.[202] It is concerning enough that the IRS would take the extreme step of visiting someone's home on the day he testified before Congress. But the IRS compiled its information from a data broker, potentially accessing vast amounts of Taibbi's private information.

These actions allow government agencies and law enforcement to evade the Fourth Amendment and collect limitless information of Americans. The Fourth Amendment Is Not For Sale Act closes this legal loophole and stops data brokers from buying and selling Americans' personal information to the government by requiring the government to obtain a court order before acquiring customer or subscriber information from a third party.

As technology continues to advance and Americans incidentally share more data through the devices we use every day, it is important for Congress to protect privacy interests and ensure that government agencies and law enforcement abide by the Fourth Amendment. Congress has the opportunity to codify the Supreme Court's decision in *Carpenter* and address "additional

---

[195] *See* Alex Deise, *Bill of the Month: The Fourth Amendment is Not for Sale Act*, FREEDOMWORKS (Jul. 29, 2022), https://www.freedomworks.org/bill-of-the-month-july-2022-the-fourth-amendment-is-not-for-sale-act/.
[196] *See* Byron Tau, *FBI Once Bought Mobile-Phone Data for Warrantless Tracking. Other Agencies Still Do.*, WALL STREET JOURNAL
[197] *Id.*
[198] *See* Laura Hecht-Felella, *Federal Agencies Are Secretly Buying Consumer Data*, BRENNAN CENTER FOR JUSTICE (Apr. 16, 2021), https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data.
[199] *Id.*
[200] *Id.*
[201] *See* Letter from Rep. Jim Jordan, Chairman, H. Comm. on the Judiciary, to Hon. Daniel Werfel, Commissioner, Internal Revenue Service (May 24, 2023).
[202] *See* Yael Grauer, *Here's a Long List of Data Broker Sites and How to Opt-Out of Them*, VICE (Mar. 27, 2018).

categories of highly sensitive information that merit the protection of a warrant regardless of whether they are held by third parties."[203]

B. NEED FOR LEGISLATION

On April 27, 2023, the House Judiciary Subcommittee on Crime and Federal Government Surveillance held a hearing entitled "Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them."[204] On July 14, 2023, the Subcommittee held a second hearing entitled "Fixing FISA, Part II."[205] Both of those hearings explored the utilities of FISA and the ways in which FISA is in need of reform to better protect Americans' civil liberties from government surveillance and abuse. In considering necessary FISA reforms, several witnesses and lawmakers expressed concerns regarding recent revelations exposing the misuse of FISA authorities by government actors.[206]

On July 19, 2023, the House Judiciary Committee unanimously passed H.R. 4639, the Fourth Amendment Is Not For Sale Act.[207] During the markup of H.R. 4639, lawmakers expressed a similar concern regarding warrantless government surveillance of Americans' data.[208] Specifically, Members expressed concern about the developing practice wherein government agencies are able to exploit a legal loophole to purchase massive amounts of Americans' information from data brokers, even though that same information would ordinarily require the agency to obtain a court order if gathering the information themselves.[209]

The pervasive surveillance and misuse of FISA authorities are well-documented. For example, in 2019 and 2020, Department of Justice Inspector General Michael Horowitz exposed how the FBI violated its authorities under FISA by improperly spying on Trump campaign associates.[210] The government also conducts "backdoor searches" of Americans' communications, most of the time without obtaining a warrant. Illustratively, in 2021, the FBI queried the communications of U.S. persons over 3.3 million times.[211] In 2022, the FBI similarly conducted hundreds of U.S. person queries per day.[212] These queries included Members of

---

[203] *Id.*
[204] *Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them: Hearing Before the Subcomm. On Crime and Fed. Gov't Surveillance*, 117th Cong. (2023).
[205] *Fixing FISA, Part II: Hearing Before the Subcomm. On Crime and Fed. Gov't Surveillance*, 117th Cong. (2023).
[206] *See id.*
[207] *Markup of H.R. 1531, H.R. 4250, and H.R. 4639 Before the H. Comm. On the Judiciary*, 118th Cong. (2023).
[208] *See generally id.*
[209] *Id.*
[210] *See, e.g.,* U.S. DEP'T. OF JUSTICE, OFFICE OF INSPECTOR GEN., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION (2019); *see also* U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GEN., MANAGEMENT ADVISORY MEMORANDUM FOR DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION REGARDING THE EXECUTION OF WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS at 3 (2020).
[211] *See generally* 2021 ODNI Annual Statistical Transparency Report, *supra* note 844.
[212] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT, CALENDAR YEAR 2022 at 24.

Congress, state senators, judges, campaign donors, protestors, and others.[213] With respect to the practice of data purchasing, several law enforcement agencies and reports have revealed the purchase of Americans' information in bulk, including the FBI, CBP, ICE, Secret Service, and DOD.[214]

H.R. 6570, the Protect Liberty and End Warrantless Surveillance Act, would put important guardrails in place to limit government surveillance and protect Americans' civil liberties. The bill requires a court order from the FISC or a warrant before any member of the intelligence community is able to query U.S. persons' information held in the Section 702 database, subject to limited exceptions. In addition, the bill drastically reduces the number of FBI officials authorized to conduct such queries. Moreover, its provisions limit the use of information obtained pursuant to Section 702, repeals the ability of the intelligence community to resume "abouts" collection, and makes important reforms to the FISC that ensure the court, and the proceedings before it, are carried out with greater transparency, integrity, and accountability. The bill also provides Congress with greater oversight of the FISC and FISCR, as well as more visibility into the intelligence community's compliance with FISA. It also eliminates the legal loophole that federal agencies use to purchase data on Americans by requiring the government to obtain a court order before acquiring such information from a third party.

Hearings

For the purposes of clause 3(c)(6)(A) of House rule XIII, the following hearings were used to develop H.R. 6570: "Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them" a hearing held on April 27, 2023, before the Subcommittee on Crime and Federal Government Surveillance of the Committee on the Judiciary. The Committee heard testimony from the following witnesses:

- Mr. Michael Horowitz, Inspector General, U.S. Department of Justice Office of the Inspector General;
- Ms. Sharon Bradford Franklin, Chair, Privacy and Civil Liberties Oversight Board; and
- Ms. Beth A. Williams, Board Member, Privacy and Civil Liberties Oversight Board.

The hearing addressed the use of FISA authorities and non-compliance with established statutory and administrative procedures intended to safeguard Americans' civil liberties.

---

[213] *See, e.g.,* Memorandum Opinion and Order, *Document re: Section 702 2021 Certification* at 29 (FISA Ct. Apr. 21, 2022).

[214] *See* Laura Hecht-Felella, *Federal Agencies Are Secretly Buying Consumer Data, Brennan Center for Justice* (Apr. 16, 2021), https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data; Byron Tau, *FBI Once Bought Mobile-Phone Data for Warrantless Tracking. Other Agencies Still Do.*, Wall Street Journal

The Subcommittee on Crime and Federal Government Surveillance also held a hearing on July 14, 2023, titled "Fixing FISA, Part II." The Committee heard testimony from the following witnesses:

- Professor Jonathan Turley, George Washington University Law School;
- Mr. Phil Kiko, Principal, Williams & Jensen;
- Mr. Gene Schaerr, General Counsel, Project for Privacy and Surveillance Accountability; and
- Ms. Elizabeth Goitein, Senior Director, Liberty & National Security Program, Brennan Center for Justice.

The hearing further addressed the deficient safeguards in FISA, and contemplated the necessity of imposing a warrant requirement for Section 702 queries.

Committee Consideration

On December 6, 2023, the Committee met in open session and ordered the bill, H.R. 6570, favorably reported with an amendment in the nature of a substitute, by a roll call vote of 35 to 2, a quorum being present.

Committee Votes

In compliance with clause 3(b) of House rule XIII, the following roll call votes occurred during the Committee's consideration of H.R. 6570:

1. Vote on Amendment #3 to H.R. 6570 ANS, offered by Mr. Swalwell, failed 9-20
2. Vote on Amendment #4 to H.R. 6570 ANS, offered by Mr. Buck, failed 4-22
3. Vote on Favorably Reporting H.R. 6570, as amended, passed 35-2

[INSERT "B" - ROLL CALL VOTE SHEETS]

Committee Oversight Findings

In compliance with clause 3(c)(1) of House rule XIII, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

New Budget Authority and Tax Expenditures

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the *Congressional Budget Act of 1974* and with respect

to the requirements of clause 3(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the *Congressional Budget Act of 1974*, the Committee has requested but not received a cost estimate for this bill from the Director of the Congressional Budget Office. The Committee has requested but not received from the Director of the Congressional Budget Office a statement as to whether this bill contains any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures. The Chairman of the Committee shall cause such estimate and statement to be printed in the *Congressional Record* upon its receipt by the Committee.

Congressional Budget Office Cost Estimate

With respect to the requirement of clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, a cost estimate provided by the Congressional Budget Office pursuant to section 402 of the *Congressional Budget Act of 1974* was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the *Congressional Record* upon its receipt by the Committee.

Committee Estimate of Budgetary Effects

With respect to the requirements of clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the *Congressional Budget Act of 1974*.

Duplication of Federal Programs

Pursuant to clause 3(c)(5) of House rule XIII, no provision of H.R. 6570 establishes or reauthorizes a program of the federal government known to be duplicative of another federal program.

Performance Goals and Objectives

The Committee states that pursuant to clause 3(c)(4) of House rule XIII, H.R. 6570 reauthorizes Section 702 of the Foreign Intelligence Surveillance Act (FISA) for three years with significant reforms. It requires the government to obtain an order from the Foreign Intelligence Surveillance Court (FISC) or a warrant prior to conducting U.S. person queries of information collected through Section 702. It provides for greater scrutiny of applications submitted to the FISC, increases transparency in surveillance applications, requires more frequent and detailed reports and audits, and establishes additional penalties for government employees who violate FISA or mislead the FISC.

The bill also closes the legal loophole that allows data brokers to sell Americans' personal information to law enforcement, intelligence agencies, and other government agencies without the agency first acquiring a warrant. If the agency were to gather this information itself,

it would be required to obtain a warrant, subpoena, or other legal order. By closing this loophole, the bill prevents government agencies from conducting an end-run around the protections of the Fourth Amendment.

Advisory on Earmarks

In accordance with clause 9 of House rule XXI, H.R. 6570 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clauses 9(d), 9(e), or 9(f) of House Rule XXI.

Federal Mandates Statement

An estimate of federal mandates prepared by the Director of the Congressional Budget office pursuant to section 423 of the *Unfunded Mandates Reform Act* was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the *Congressional Record* upon its receipt by the Committee.

Advisory Committee Statement

No advisory committees within the meaning of section 5(b) of the *Federal Advisory Committee Act* were created by this legislation.

Applicability to Legislative Branch

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the *Congressional Accountability Act* (Pub. L. 104-1).

Correspondence

[INSERT C – COMMITTEE LETTERS]

Section-by-Section Analysis

Sec. 1. Short Title.

- The Act is the "Protect Liberty and End Warrantless Surveillance Act."

Sec. 2. Query Procedure Reform.

- Limits the number of FBI employees who may perform United States person queries to 5 employees per field office.

- Limits the number of FBI employees at FBI headquarters who may perform U.S. person queries to 5.

- Prohibits U.S. person queries of Section 702-acquired information if the compelled production of that information would require a probable cause warrant if sought for law enforcement purposes in the United States.

    - Provides an exception when the subject of a query is subject to an order or emergency authorization under Title I or Title III of FISA, or a criminal warrant.

    - Provides an exception when there is a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm and the information is sought for the purpose of preventing or mitigating the threats. Requires a description of the query to be sent to FISC, House and Senate Judiciary Committees, and House and Senate Intelligence Committees.

    - Provides an exception where the U.S. person gives consent to the query.

    - Provides an exception where the query uses a known cybersecurity threat signature as a query term, and query is conducted for sole purpose of mitigating or preventing such a threat. Requires these queries to be reported to the Foreign Intelligence Surveillance Court (FISC).

- Permits queries for communications metadata but prohibits use of results of a metadata query as a basis for access to communications and other protected information.

- Requires that queries must be reasonably likely to retrieve foreign intelligence information.

- For all U.S. person queries, requires documentation of the query term, date of query, identifier for person conducting query, and statement of facts showing that query was reasonably likely to retrieve foreign intelligence information or in furtherance of the exceptions.

Sec. 3. Limitation on Use of Information Obtained Under Section 702 of the Foreign Intelligence Surveillance Act of 1978 Relating to United States Persons and Persons Located in the United States in Criminal, Civil, and Administrative Actions.

- Prohibits the use in criminal, civil, and administrative proceedings and investigations, of information acquired under section 702, except with prior approval of the Attorney General and provided that the proceeding or investigation involves terrorism, actions necessitating counterintelligence, the proliferation or use of a weapon of mass destruction, a cybersecurity breach or attack from a foreign country, incapacitation or destruction of critical infrastructure, an attack against the armed forces of the United States or an ally of the United

States or to other personnel of the United States Government or a government ally of the United States, or international narcotics trafficking.

Sec. 4. Repeal of Authority For the Resumption of Abouts Collection.

- Repeals the authority to resume "abouts" collection under Section 702. Existing law permits the resumption of "abouts" collection with notice to Congress.

Sec. 5. Foreign Intelligence Surveillance Court (FISC) Reform.

- Requires the same FISC judge to hear FISA renewal applications unless that judge is no longer serving on the FISC.

- Allows the FISC to appoint one or more amicus curiae in a case and expands the types of cases where the FISC shall appoint an amicus curiae, unless the court issues a finding that such appointment is not appropriate. Such cases would include: A case that presents a novel or significant interpretation of the law (current law only provides for amicus participation in these such cases); a case that presents significant concerns with respect to the activities of a U.S. person that are protected by the First Amendment of the Constitution; a case that presents or involves a Sensitive Investigative Matter; a case that presents a request for approval of a new program, a new technology, or a new use of existing technology; a case that presents a request for reauthorization of programmatic surveillance; a case that otherwise presents novel or significant civil liberties issues; and a case that involves the activities of a U.S. person.

- Defines Sensitive Investigative Matter (SIM) to be an investigative matter involving the activities of: a domestic public official or political candidate, or a staff member of such an official or candidate; a domestic religious or political organization, or a U.S. person prominent in such an organization; or the domestic news media.

    - SIM also includes "any other investigative matter involving a domestic entity or a known or suspected U.S. person that," in the judgment of the applicable court, is as sensitive as a Sensitive Investigative Matter.

- Grants amici the authority to seek review of FISC decisions to the United States Foreign Intelligence Surveillance Court of Review (FISCR) and of FISCR decisions to the United States Supreme Court, and requires the FISC to provide a written statement of reasons for a denial of a petition for review by an amicus.

- Provides amici with access to certain documents in connection with the matter, including classified information.

Sec. 6. Application for an Order Approving Electronic Surveillance.

- Requires the application to include a statement describing the normal investigative techniques taken before submitting the application and an explanation as to why those techniques are insufficient.

- Applications for electronic surveillance must include all information material to an application, including exculpatory information.

- Each federal employee who contributes to the drafting of a FISA application must sign an affidavit attesting to the accuracy of the application.

- Prohibits the use of opposition research and news media in FISA applications unless that information disclosed in the application and provided that it is not the sole source of the information justifying the allegations in the application.

Sec. 7. Public Disclosure and Declassification of Certain Documents.

- Currently, 50 U.S.C. 1871(c) requires the Attorney General to share with the House and Senate Intelligence and Judiciary Committees certain FISC decisions, orders, and opinions within 45 days of issuance. This provision would require that the Attorney General also share copies of those documents that have undergone declassification review at that same time.

- Amends 50 U.S.C. 1872(a) to require the Director of National Intelligence and Attorney General to conclude their declassification review not later than 45 days after commencement of such review.

Sec. 8. Transcriptions of Proceedings; Attendance of Certain Congressional Officials at Certain Proceedings.

- Allows the Chair and Ranking Member of the House and Senate Judiciary Committees and the House and Senate Intelligence Committees, or their designated staff, to attend all FISC and FISCR proceedings. Allows the Chairs and Ranking Members to designate 2 Members of Congress to attend proceedings on their behalf.

- Requires transcripts of FISC proceedings to be maintained and available for review by those permitted to attend proceedings not later than 45 days after any such proceedings.

Sec. 9. Annual Audit of FISA Compliance by Inspector General.

- Requires the DOJ IG to complete an annual report of alleged violations and failures to comply with the requirements of FISA and to submit that report to the congressional intelligence committees and House and Senate Judiciary Committees by June 30 of each year.

Sec. 10. Reporting on Accuracy and Completeness of Applications.

- Requires an existing annual report by the Director of the Administrative Office of the United States Courts to include an additional analysis of the accuracy and completeness of applications and certifications.

Sec. 11. Annual Report of the Federal Bureau of Investigation.

- Requires the FBI to annually report to Congress a comprehensive account of ongoing disciplinary investigations, adjudication of concluded investigations, and subsequent disciplinary actions resulting from violations of the requirements of FISA.

- Requires the FBI to annually report to Congress on the number of U.S. person queries conducted, what terms were used, the number of warrants issued and denied, and the number of times exceptions from the warrant requirement were alleged.

Sec. 12. Extension of Title VII of FISA; Expiration of FISA Authorities; Effective Dates.

- Extends Title VII (including Section 702 of FISA) for 3 years, until December 31, 2026.

Sec. 13. Criminal Penalties for Violations of FISA.

- Increases the maximum penalty for a person who intentionally engages in electronic surveillance under color of law or intentionally discloses or uses information obtained under color of law by electronic surveillance not authorized by law. Makes these offenses punishable by a fine of not more than $10,000 or imprisonment of not more than 8 years, or both.

- Adds criminal penalty for knowingly making a false material declaration or material omission in any document submitted to or statement made before the FISC or FISCR. Makes this offense punishable by a fine of not more than $10,000 or imprisonment for not more than 8 years, or both.

- Adds criminal penalty for intentionally disclosing a FISA application or classified information contained in the application to any person not entitled to receive such information. Makes this offense punishable by a fine of not more than $10,000 or imprisonment for not more than 8 years, or both.

Sec. 14. Contempt Power of FISC and FISCR.

- Provides FISC and FISCR with the authority to prosecute a person for contempt and requires the FISC and FISCR to jointly submit an annual report to Congress on the use of this authority.

Sec. 15. Increased Penalties for Civil Actions.

- Increases civil damages for a U.S. person harmed by a violation of FISA to $10,000 (current statute is $1,000 for an aggrieved person).

- If a court finds a person violated the Act, the head of the agency that employs that person shall submit a report to Congress on the administrative action taken against that person and report their name to the FISC.

Sec. 16. Accountability Procedures for Incidents Relating to Queries Conducted by the FBI.

- Requires the Director of the FBI to establish procedures to hold FBI employees accountable for violations of law, guidance, and procedures governing queries of Section 702-acquired information.

- The accountability procedures shall include centralized tracking of incidents, minimum consequences for initial and subsequent incidents. Includes a clarification for requirements for referring intentional misconduct and reckless conduct to the FBI's Inspection Division for investigation and disciplinary action by the FBI's Office of Professional Responsibility.

- Requires a report to Congress detailing the accountability procedures and an annual report describing disciplinary actions taken and a description of the circumstances surrounding each such disciplinary action.

Sec. 17. Agency Procedures to Ensure Compliance.

- Requires each agency that acquires foreign intelligence information under FISA to establish clear rules on what constitutes a violation of the Act, and procedures for taking appropriate adverse personnel actions against any officer or employee who engages in such a violation, including more severe adverse actions for any subsequent violation. Requires the head of each federal department or agency to report to Congress on such procedures not later than 3 months after the date of enactment.

Sec. 18. Protection of Records Held By Data Brokers.

- Defines various terms and prevents law enforcement and intelligence agencies from buying data about a United States person, located anywhere in the world, or data about any person located in the United States that:

- Is data about a person's device, from their online account, or created or shared by a technology and telecommunications company providing a service to that person;

- Was obtained from a technology or communications company providing service to the target in a manner that violated a contract, or the company's terms of service or privacy policy;

- Was obtained by deceiving the person whose information was obtained; or

- Was obtained by accessing the person's device or online account without authorization.

- Also prohibits the use or sharing by the government of any information obtained in violation of this section, including as evidence in court or before a grand jury, regulatory body, or in another similar proceeding. This section further requires the Attorney General to adopt specific procedures to minimize the acquisition and retention of this information, and to prohibit its dissemination.

Sec. 19. Required Disclosure.

- Prohibits the use or sharing by the government of any information obtained in violation of this section, including as evidence in court or before a grand jury, regulatory body, or in another similar proceeding. This section further requires the Attorney General to adopt specific procedures to minimize the acquisition and retention of this information, and to prohibit its dissemination.

Sec. 20. Intermediary Service Providers.

- Extends the protections in the Electronic Communications Privacy Act to data held by intermediary service providers, which are entities that directly or indirectly deliver, store, or process communications for or on behalf of technology or communications firms.

Sec. 21. Limits on Surveillance Conducted for Foreign Intelligence Purposes Other than Under the Foreign Intelligence Surveillance Act of 1978.

- Narrows a legal carveout in FISA permitting the intelligence community, without an order issued by a court, to buy or obtain through other methods, metadata about calls, texts, emails, and web browsing, where at least one end of the communication is located abroad. This section limits the carveout such that it only applies to the acquisition of foreign intelligence information of non-Americans located outside the United States.

- Specifies that FISA authorities shall be the exclusive means by which the government obtains information inside the U.S. or from U.S. technology or communications companies electronic communications transactions records, call detail records, or other metadata about

the communications of United States persons, located anywhere in the world, or any person located in the United States.

- Specifies that Title I and sections 303, 304, 703, 704, and 705 of FISA shall be the exclusive means by which the government obtains inside the location information of U.S. persons or persons inside the United States, web browsing history, Internet search history, or any other data that would require a court order to compel, about United States persons, located anywhere in the world, or any person located in the United States.

Sec. 22. Limit on Civil Immunity for Providing Information, Facilities, or Technical Assistance to the Government Absent a Court Order.

Removes the Attorney General's authority to grant civil immunity to those that provide unlawful assistance for government surveillance not required or permitted by federal law. Immunity remains for any surveillance assistance ordered by a court.

Sec. __. Prohibition on Reverse Targeting of United States Persons and Persons Located in the United States

Prohibits the acquisition of communications if a significant purpose is to acquire the information of one or more United States person or persons believed to be located in the United States.

Sec. __. Required Disclosure of Relevant Information in Foreign Intelligence Surveillance Act of 1978 Applications

Requires the Attorney General to establish a set of accuracy procedures to ensure that an application for a court order under FISA includes all information that might reasonably call into question the accuracy of the information or reasonableness of any assessment in the application. Requires the application to include a description of the accuracy procedures and a certification that the federal officer making the application has reviewed it for accuracy and completeness.

Sec. __. Enhanced Annual Reports by Director of National Intelligence

Requires enhanced reports on statistics regarding persons targeted for surveillance under Section 702, and other reports including the number of disseminated intelligence reports derived from collection pursuant to section 702 containing the identities of U.S. persons, the number of disseminated intelligence reports derived from collection not authorized by FISA containing the identities of U.S. persons, the number of queries conducted to find communications or information of or about U.S. persons, the number of criminal proceedings in which the government entered into evidence or otherwise used or disclosed in a criminal proceeding any information obtained or derived from an acquisition conducted without a court order, subpoena, or other legal process established by statute.

Sec. __. Quarterly Report

Requires the Attorney General, in consultation with the Director of National Intelligence, to submit quarterly reports to the congressional intelligence committees and Committees on the Judiciary of the Senate and of the House of Representatives that include the total number of warrants issued to conduct a query of information acquired under section 702, the total number of times a query was conducted pursuant to an exception, the total number of queries that were conducted using a United States person query term.

Changes in Existing Law Made by the Bill, as Reported

[INSERT "D" – PREPARED BY LEG. COUNSEL]