The Security And Freedom Enhancement Act of 2024

Sec. 1. Short Title.

- The Act is the "SAFE Act of 2024."

Title I—Protections for United States Persons Whose Communications Are Collected Under Section 702 of the Foreign Intelligence Surveillance Act of 1978

Sec. 101. Query Procedure Reform.

Even though Section 702 surveillance may only be targeted at foreigners overseas, intelligence agencies have used Section 702 to surveil Americans whose communications have been swept up by Section 702 collection. It has been used to conduct improper searches for the private communications of protesters, members of Congress, journalists, and political donors. Each of the provisions in this section is intended to prevent future abuses of Section 702 and protect Americans from warrantless searches. In particular, the probable cause court order requirement will prevent agencies from accessing the contents of Americans' communications without first obtaining individualized approval from a judge. To ease the burden on both the government and the courts, this provision only requires the government to obtain such approval to access the results of a U.S. person query. Because only a small percentage of U.S. person queries return results, this compromise approach dramatically reduces the administration burden of obtaining court approval. Specifically, Section 101:

- Enhances internal oversight of FBI queries by requiring:
  - DOJ audits every 180 days of a representative sample of U.S. person queries performed by the FBI;
  - annual training for FBI personnel conducting queries;
  - approval from the Deputy Director of the FBI for any query involving a U.S. elected official, a U.S. or state political appointee, a U.S. political organization or U.S. person prominent in such organization, or a U.S. media organization or U.S. person member of such organization;
  - FBI attorney approval for any query involving a U.S. religious organization or U.S. person prominent in such organization, or for any "batch" query;
  - prior written justification for U.S. person queries; and
  - querying systems that require FBI agents to "opt in" to including Section 702 data when running a query against systems that include data from multiple sources.

- Requires government officials to have a foreign intelligence purpose for conducting U.S. person queries of Section 702 data, with exceptions for:
  - exigent circumstances;
  - consent; or
  - queries designed to identify targets of cyberattacks.

- Requires government officials to obtain warrants or FISA Title I orders before accessing content returned by a U.S. person query (but not before conducting the query), with exceptions for:
  - exigent circumstances (i.e., the official performing the search reasonably believes that there is an imminent threat of death or serious bodily harm, and the information is sought for the purpose of preventing or mitigating the threat);
  - consent (e.g., where the subject of the search is a potential victim or target of a foreign plot); or
  - queries designed to identify targets of cyberattacks, where the only content accessed and reviewed is malicious software or cybersecurity threat signatures.

- For all cases in which content is accessed as a result of a U.S. person query, requires the official or employee accessing the content to create an electronic record that includes a statement of facts showing that a warrant/Title I order was obtained or that an exception applies.

Sec. 102. Quarterly Reports.

- Requires the Attorney General, in consultation with the Director of National Intelligence, to submit quarterly reports to the congressional judiciary and intelligence committees setting forth the total number of U.S. person queries conducted of information acquired under Section 702; the number of times such queries resulted in government officials accessing content; the number of times a warrant or FISA Title I order was obtained to access content; and the number of times content was accessed pursuant to one or more specified statutory exceptions. These reports will give Congress critical feedback on how and whether the government is implementing the provisions of Section 101.

Sec. 103. 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 must include centralized incident tracking and minimum consequences for initial and any subsequent incidents. Includes a clarification that intentional misconduct and reckless conduct must be referred to the FBI's Inspection Division for investigation and disciplinary action by the FBI's Office of Professional Responsibility. This provision is intended to ensure that FBI employees are held appropriately accountable for abusing their access to Section 702 information.

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

Sec. 104. Prohibition on Reverse Targeting of United States persons and persons located in the United States.

- Strengthens and clarifies the existing prohibition on "reverse targeting" by prohibiting the warrantless acquisition of communications under Section 702 if "a significant purpose"—rather than "the purpose"—is to target a United States person or person reasonably believed to be located in the United States.

Sec. 105. FISA Court Review of Targeting Decisions.

- Helps to ensure compliance with Section 702 targeting requirements and with prohibition on reverse targeting by requiring the FISC to review a random sample of past targeting decisions and supporting documentation on an annual basis.

Sec. 106. Repeal of Authority for the Resumption of Abouts Collection.

- Repeals the authority to resume "abouts" collection under Section 702. "Abouts" collection was a practice under which the NSA collected communications "about" a particular target, rather than just to or from the target; among other issues, it routinely resulted in the collection of large numbers of purely domestic communications. The NSA ended "abouts" collection in 2017 after it could not find a way to continue it that was consistent with the requirements of Section 702. Existing law, however, permits the resumption of "abouts" collection with advance notice to Congress.

Sec. 107. Extension of Title VII of FISA; Expiration of FISA Authorities; Effective Dates.

- Extends Title VII (including Section 702 of FISA) until December 31, 2027. This extension of nearly four years is aligned with past extensions, which have ranged from four to six years. It is on the shorter end of those past extensions because of the extent of recent abuses and because the bill makes changes to the law that should be evaluated in the near term.

Title II—Additional Reforms Relating to Activities Under the Foreign Intelligence Surveillance Act

Sec. 201. Application for an Order Approving Electronic Surveillance.

The provisions of this section are designed to improve the accuracy of applications to conduct surveillance, bolster FISC scrutiny of applications, and ensure that there is sufficient justification when the government seeks to conduct surveillance of Americans.

- Requires the government, in its surveillance applications, to describe the investigative techniques it has employed prior to seeking a surveillance order.
- Requires the government, when seeking to renew a surveillance order, to describe the foreign intelligence information acquired under the original order or explain the failure to acquire foreign intelligence information under that order.

- Strengthens existing requirements that U.S. persons who are subject to surveillance as "agents of a foreign power" must be engaged in criminal activity.
- Requires the Attorney General to adopt procedures to ensure the accuracy of FISA applications; requires officials applying for FISA orders to certify that accuracy procedures have been followed; requires the FISC to find that accuracy procedures meet the criteria for such procedures set forth in the statute.
- Requires the government to disclose to the FISC all information that is material to the Court's determination, including exculpatory information.
- Prohibits the government, in submitting applications for FISA surveillance, from relying on information obtained from the content of a media source unless the government discloses the source and explains the investigative techniques it used to try to corroborate the information.
- Prohibits the government, in submitting applications for FISA surveillance, from relying on information gathered by a political campaign unless the government discloses the source and the political campaign is not the sole source of the information.

Sec. 202. Criminal Penalties for Violations of FISA.

- Helps to deter intentional abuses of FISA by—
  - increasing the maximum penalty for government employees who abuse their power to perform electronic surveillance, including by leaking surveillance information;
  - making it a crime to knowingly make a material false statement or omission on any document submitted to the FISC or FISCR; and
  - making it a crime to leak applications to the FISC or classified information contained in those applications.

- Each of these offenses is punishable by a fine of not more than $10,000 or imprisonment of not more than 8 years, or both.

Sec. 203. Increased Penalties for Civil Actions.

- Increases civil damages for a U.S. person harmed by a violation of FISA to $10,000 (from $1,000) and requires agencies to report to Congress and the FISC if a court finds that one of the agency's employees violated FISA. This provision will help ensure that civil damages reflect the harm done by abusive surveillance, and will aid Congress and the FISC in overseeing the implementation of FISA.

Sec. 204. Agency Procedures to Ensure Compliance.

While Section 202 requires specific accountability measures for violations relating to the queries of Section 702-acquired data, this section includes a more general accountability requirement for all FISA violations to help ensure that agencies respond appropriately when employees abuse their access to sensitive intelligence information.

- Requires each agency that acquires foreign intelligence information under FISA to establish clear rules on what constitutes a violation of the Act, as well as procedures for taking

appropriate adverse personnel actions against any officer or employee who engages in such a violation, including escalating consequences for subsequent violations.

- Requires the head of each federal department or agency to report to Congress on the implementation of such procedures within three months of enactment.

Sec. 205. 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 or undertaken on a temporary basis pursuant to an emergency authorization. This provision will incentivize electronic communication service providers to ensure that they only comply with lawful demands for assistance from the government.

Title III—Reforms Relating to Proceedings Before the Foreign Intelligence Surveillance Court and Other Courts

Sec. 301. Foreign Intelligence Surveillance Court (FISC) Reform.

- Prohibits "judge shopping" by requiring the same FISC judge to hear applications for renewals of an order approving FISA surveillance unless that judge is no longer serving on the FISC.

- Incorporates the Lee-Leahy Amendment, which passed the Senate 77–19 in 2020, to strengthen the role of the FISC amici. That amendment—
  - Expands the types of cases in which the FISC is required to appoint an amicus curiae (unless the court issues a finding that such appointment is not appropriate) to include cases involving Americans' First Amendment rights; cases involving investigations of politicians and their staff, religious figures, or members of the media; cases involving new technologies or surveillance programs; cases involving requests to engage in programmatic surveillance; and all other cases that present novel or significant civil liberties issues.
  - Grants amici the authority to petition the FISC to certify its decisions for review the United States Foreign Intelligence Surveillance Court of Review (FISCR), and to petition the FISCR to certify its decisions for review by the United States Supreme Court; requires the FISC to provide a written statement of reasons for denying any such petition. The law currently gives amici no authority to seek appellate review of adverse decisions, even though the government has this power.
  - Ensures that security-cleared amici have access to all information necessary to adequately represent the public's interests in the matter.

- Allows an amicus curiae to consult with one or more of the other individuals designated by the court to serve as amicus curiae regarding any of the information relevant to any assigned proceeding.

Sec. 302. Public Disclosure and Declassification of Certain Documents.

Currently, 50 U.S.C. § 1872 requires the Attorney General, in consultation with the Director of National Intelligence, to conduct a declassification review of significant FISC decisions and make the decisions public to the maximum extent possible. However, the law does not specify a time period in which the declassification review must be conducted, and the government has taken a year or longer to declassify FISC opinions that reveal significant government violations. This provision requires the declassification review to be completed within 180 days of the decision's issuance, thus ensuring greater transparency for FISC proceedings and preventing the government from delaying the release of damaging information.

Sec. 303. Submission of Court Transcripts to Congress.

- Requires any transcripts of FISC proceedings to be provided to congressional intelligence and judiciary committees within 45 days after the government's receipt of the transcript. This provision will ensure greater transparency of FISC proceedings, allowing Congress to better oversee the implementation of FISA.

Sec. 304. Contempt Power of FISC and FISCR.

- Provides FISC and FISCR with the authority to punish a person for contempt and requires the FISC and FISCR to jointly submit an annual report to Congress on the use of this authority. This provision will help deter government officials from misleading the FISC and will allow appropriate punishment for those who do.

Title IV—Independent Executive Branch Oversight

Sec. 401. Periodic Audit of FISA Compliance by Inspector General.

- Requires the DOJ Inspector General to complete a report every five years on alleged or potential violations and failures to comply with the requirements of FISA, including an analysis of the accuracy and completeness of applications and certifications submitted to the FISC, and to submit that report to the congressional judiciary and intelligence committees. This will provide Congress with critical information on an ongoing basis about any problems with the operation of FISA, including Section 702.

Sec. 402. Intelligence Community Parity and Communications with Privacy and Civil Liberties Oversight Board.

- The Privacy and Civil Liberties Oversight Board plays a key role in ensuring that counterterrorism programs respect Americans' civil liberties. But current law does not protect whistleblowers who report government misconduct to the Board, even though it protects disclosures to other overseers (e.g., inspectors general). Moreover, Board members' salaries have not kept pace with the intelligence officials whose conduct they oversee. This provision addresses these problems by adding the Board to the list of entities to whom intelligence community whistleblowers can make protected disclosures under the law, and by ensuring that Board members are compensated in a manner that is consistent with comparable positions within the Intelligence Community.

Title V—Protections for United States Persons Whose Sensitive Information Is Purchased by Intelligence and Law Enforcement Agencies

Sec. 501. Prohibition on Intelligence Acquisition of United States Person Data.

Sections 501 and 502 are designed to address the data broker loophole, under which intelligence and law enforcement agencies are increasingly evading constitutional and statutory privacy protections by purchasing highly sensitive information that would otherwise require a warrant, court order, or subpoena to obtain. Intelligence agencies and law enforcement agencies are addressed in separate sections to reflect their differing collection practices. Section 501—

- Prohibits an element of the intelligence community from acquiring Americans' sensitive personal information, unless the agency has obtained an order or emergency authorization under FISA or Title 18.

- Does not apply to data that is:

    - lawfully available to the public through Federal, State, or local government records or through widely distributed media;
    - reasonably believed to have been voluntarily made available to the general public by the covered person; or
    - obtained through the collection of a specific transaction or communication between an American and a non-American who is the intended target of the surveillance.

- Includes multiple commonsense exceptions that allow agencies to acquire data without a court order for employment-related purposes; for purposes of supporting compliance with applicable laws or regulations; to respond to an emergency involving a threat of death or serious bodily harm; or with the consent of the person whose data is acquired. For each of these exemptions, the data may only be used for that specific purpose and must be destroyed when it is no longer necessary for that purpose.

- Allows agencies to acquire datasets that include Americans' sensitive data without a court order if the agencies cannot identify or exclude such data prior to collection or operational

use of the dataset, as long as the agencies follow strict minimization procedures. Under those procedures, retention and querying of incidentally collected data are permitted only to the extent the information would fall within one of the exceptions to the prohibition on collection.

- Prohibits use in investigations or legal proceedings of data acquired in violation of this section.

- Requires a report to Congress from the Director of National Intelligence on the acquisition of datasets that the Director anticipates will contain information on Americans that is significant in volume, proportion, or sensitivity, as well as of requiring the DNI to notify Congress of changes to the information in the report. Unclassified versions of the report and notifications must be made public.

Sec. 502. Limitations on Law Enforcement Purchase of Personal Data from Data Brokers.

- Prohibits law enforcement agencies from purchasing Americans' sensitive information and prohibits other agencies that purchase Americans' sensitive information from sharing it with law enforcement agencies.

- Does not apply to data that is:

    - lawfully available to the public through Federal, State, or local government records or through widely distributed media;
    - reasonably believed to have been voluntarily made available to the general public by the covered person; or
    - obtained through the collection of a specific transaction or communication between an American and a non-American who is the intended target of the surveillance.

- Includes multiple commonsense exceptions that allow agencies to:
    - provide compensation when obtaining data through compulsory legal process;
    - provide a payment or bounty for information obtained pursuant to a statutorily authorized whistleblower program; and
    - purchase data for employment-related purposes; for the purpose of conducting background checks; to respond to an emergency involving a threat of death or serious bodily harm; for purposes of supporting compliance with applicable laws or regulations; or with the consent of the person whose data is acquired.

  For each of these exceptions, the data may only be used for that specific purpose and must be destroyed when it is no longer necessary for that purpose.

- Allows agencies to acquire datasets that include Americans' sensitive data without a court order if the agencies cannot identify or exclude such data prior to collection or operational use of the dataset, as long as the agencies follow strict minimization procedures. Under those procedures, retention and querying of incidentally collected data are permitted only to the extent the information would fall within one of the exceptions to the prohibition on collection.

- Prohibits use in investigations or legal proceedings of data acquired in violation of this section.

Sec. 503. Consistent Privacy Protections for Demands for Data Held by Interactive Computing Services.

- Updates the Electronic Communications Privacy Act by requiring law enforcement to follow the same procedures currently required for obtaining data from providers of "electronic communication services" or "remote computing services" when obtaining similar data held by "interactive computing services"—that is, the websites and apps that Americans use every day.

Sec. 504. Consistent Privacy Protections for Data Held by Data Brokers.

- Prohibits intelligence and law enforcement agencies from compelling covered organizations such as data brokers to produce information without obtaining an order on the same basis and subject to the same limitations as an order to demand data from an online service provider. This provision ensures that Americans' private information is protected, regardless of who holds it, and will end the practice of agencies using data brokers to make an end-run around existing privacy law.

Sec. 505. Protection of Data Entrusted to Intermediary or Ancillary Service Providers.

- Extends the protections in the Electronic Communications Privacy Act to data held by intermediary and ancillary service providers, which are entities that directly or indirectly deliver, store, or process communications for or on behalf of technology or communications firms. This provision updates ECPA to account for changing technology since the law was enacted, which allows companies other than the direct service provider to have access to Americans' sensitive communications.

Title VI—Transparency

Sec. 601. Enhanced Annual Reports by Director of National Intelligence.

- Bolsters existing reporting requirements by requiring additional information and statistics to give Congress and the public a clearer understanding of how the government uses Section 702, data broker purchases, and other intelligence authorities to obtain information about Americans. Additional reporting requirements include—
  - a description of the subject matter of certifications issued under Section 702 (which the government disclosed for the first time last year);
  - the number of persons targeted for surveillance under Section 702, broken down by the certification under which the person was targeted;
  - the number of directives issued under Section 702, broken down by the type of provider receiving the directive;

- the number of disseminated intelligence reports containing information about U.S. persons, broken down by whether the information was masked or unmasked and whether it was obtained under Section 702 or under non-FISA authorities;
- the number of U.S. person queries conducted of information obtained under Attorney General-approved procedures;
- the number of criminal proceedings which made use of evidence obtained or derived from acquisition under Attorney General-approved procedures; and
- an estimate of the percentage of U.S. person communications retained under existing statutory retention limitations.

Title VII—Limited Delays in Implementation

Sec. 701. Limited Delays in Implementation

- Allows the Attorney General to delay implementation of a provision of the Act for up to one year if the intelligence communities demonstrate to the Judiciary Committees that a delay is necessary in order to comply with the changes.