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. 23. 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. 24. 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. 25. Enhanced Annual Reports by Director of National Intelligence.

- A description of the subject matter of each section 702(h) certification, requires enhanced reports on statistics regarding persons targeted for surveillance under section 702(a), and other reports including the number of disseminated intelligence reports derived from collection pursuant to section 702(i)(1), the total 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 U.S. person queries conducted without a court order, 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, good faith estimate of communications retained longer than five years.
- Removes FBI's exemption from reporting on queries.

Sec. 26. 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 or a person reasonably believed to be in the United States.