Government Surveillance Reform Act of 2026

Section 1. Short Title; Table of Contents

This section provides that the short title of this bill is the Government Surveillance Reform Act of 2026 and sets out the table of contents.

Sec. 2. Definitions.

This section defines:

- "Foreign Intelligence Surveillance Court" as the court established in section 103(a) of FISA
- "Foreign Intelligence Surveillance Court of Review" and "Court of Review" as the court established in section 103(b) of FISA
- "appropriate committees of Congress" as the congressional intelligence and judiciary committees
- "covered person" as, with respect to a query, a communication, an acquisition, or creation of information:
    - a United States person; or
    - a person known or believed to be located in the U.S. at the time of the applicable query, or at the time of communication, acquisition, or creation of information subject to the applicable query

Title I—Protections for United States persons whose communications are collected under Section 702 of the Foreign Intelligence Surveillance Act of 1978

Sec. 101. Protections related to Warrantless Queries for the Communications of United States Persons and Persons Located in the United States.

This section redefines "query" to mean the use of any terms to retrieve 702-collected information, whether manually or by automated means.

This section defines "covered query" to mean a query using a term associated with a covered person or to retrieve information of or concerning covered persons.

This section defines "covered information" to mean communications content; and other information, the compelled disclosure of which requires a probable cause warrant if sought for law enforcement purposes in the United States.

Warrant to access Americans' communications and other covered information: This section requires the government, when searching 702-collected information, to obtain a warrant, FISA court order, or FISA emergency authorization before accessing covered information returned in response to a covered query, with exceptions for:

- Exigent circumstances, with notification to the FISA Court and Congress (the official accessing the information 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 (for example, if the subject of a search is a potential victim or target of a foreign plot)
- Defensive cybersecurity purposes, with notification to the FISA Court and Congress

This prohibition does not prevent the government from conducting queries without accessing a covered persons' warrant-protected information, or from accessing communications metadata.

Foreign intelligence purpose required: This section requires all queries to be reasonably likely to retrieve foreign intelligence information and to have a significant foreign intelligence purpose for all queries, including queries for metadata, unless the existing exceptions that permit the FBI to make evidence-of-a-crime queries apply. These are:

- Emergency queries, where there is "reasonable belief that such query may retrieve information that could assist in mitigating or eliminating a threat to life or serious bodily harm"
- Preservation or production obligations in litigation, and discovery obligations in criminal matters

Documentation of accesses of covered information: This section requires that all accesses of covered information in response to a covered query are documented in an electronic record system that records:

- The date of the access
- The identifier of the officer/employee who did the particular access
    - For automated accesses, this is the officer or employee who was the proximate cause of such access
- A statement of facts showing that the access was authorized by a warrant or FISA court order/emergency authorization, or an exception

Documentation of queries: This section requires that all queries are documented in an electronic record system that records:

- Each term used for the query
- The date of the query
- The identifier of the officer/employee who conducted the query
    - For automated queries, this is the officer or employee who was the proximate cause of such query
- A statement of facts justifying the covered query would retrieve foreign intelligence information and the significant foreign purpose for the query, or the basis for an exception

Sec. 102. 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.

Current law prohibits section 702-acquired information from being used against United States persons in criminal cases, with exceptions for national security, certain serious crimes, or if the FBI obtains a FISA court order. This section extends that prohibition to all covered persons in criminal, civil, and administrative cases.

Sec. 103. Prohibition on reverse targeting of United States persons and persons located in the United States.

Existing law prohibits the intentional targeting of a non-U.S. person located outside the United States if the purpose of that acquisition is to target a particular, known person believed to be in the United States.

This section prohibits the intentional targeting of a non-U.S. person located outside the United States, if a significant purpose is to acquire the information of a particular, known covered person, with exceptions for:

- Exigent circumstances (if there is a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm to such covered person)
- Consent

Sec. 104. Data retention limits for information collected under Section 702 of the Foreign Intelligence Surveillance Act of 1978.

This section requires that the Attorney General develop and entities of the intelligence community implement procedures for destroying within five years of collection, for information acquired under section 702:

1. Any information or communication pertaining to a covered person, including an encrypted communication to or from a covered person, that has been evaluated and is not specifically known to contain foreign intelligence information; and
2. Any unevaluated information, unless it can reasonably be determined that it does not contain information pertaining to a covered person or any communication to or from a covered person (regardless of whether the communication is encrypted).

Information need not be destroyed if the Attorney General determines in writing that:

1. The information is the subject of a preservation obligation in litigation, in which case it must be used solely for that purpose and destroyed after it is no longer required to be preserved; or
2. The information is being used in a proceeding or investigation consistent with section 706(a) of FISA (as amended by Section 102 of this bill).

Sec. 105. Foreign Intelligence Surveillance Court supervision of demands for technical assistance from electronic communication service providers under Section 702 of the Foreign Intelligence Surveillance Act of 1978.

Current law requires an electronic communications service provider (ECSP) to provide the assistance necessary to accomplish an acquisition under section 702. This section requires the government to demonstrate to the FISA Court that technical assistance from an ECSP is necessary, narrowly tailored to the surveillance at issue, and does not pose an undue burden to the ECSP or its customers.

This section provides that an ECSP is not obligated to comply with a directive to provide technical assistance, unless the assistance uses a manner or method approved by the FISA Court and the FISA Court issues an order provided to the ECSP describing that technical assistance.

Sec. 106. Prohibition on warrantless acquisition of domestic communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978.

This section prohibits the government from acquiring communications under Section 702 where the sender and all intended recipients were known or believed to be located in the United States at the time of acquisition or communication.

Sec. 107. Requirement of primary foreign intelligence purpose.

Existing law requires that a significant purpose of a 702 acquisition is to obtain foreign intelligence information. This section requires that obtaining foreign intelligence information is the primary purpose.

Sec. 108. Reports to Congress on sensitive queries.

This section requires the Attorney General to annually report to the congressional intelligence and judiciary committees the number of "sensitive queries" made, as defined in section 702(f)(3)(D), disaggregated by the type of query in each subclause in the definition of sensitive queries.

Sec. 109. Repeal of expanded definition of electronic communication service provider.

In 2024, section 702 was amended to permit the government to force millions of Americans to secretly spy on its behalf. This section repeals that expansion, and invalidates any section 702 directives to that expanded group of entities.

Sec. 110. Repeal of expanded querying requirements for persons traveling to the United States.

In 2024, section 702 was expanded to require vetting of all non-United States persons traveling to the United States, without sufficient protections for the United States persons that they communicate with. This section repeals that expansion in its entirety.

Sec. 111. Four-year extension of Section 702 of the Foreign Intelligence Surveillance Act of 1978

This provision extends Section 702 until April 20, 2030.

Title II—Fourth Amendment is Not For Sale Act

Sec. 201. Prohibition on Federal law enforcement purchase of personal data from data brokers.

This section prohibits Federal law enforcement agencies from purchasing personal data about covered persons, with exceptions for:

1. Personal data that is part of a larger dataset that cannot be excluded through reasonable means through the dataset, but only if minimized in accordance with procedures issued by the Attorney General to exhaust all reasonable means to exclude covered data.
2. Personal data that is disclosed through a government whistleblower program, in which a payment or bounty is paid to the whistleblower.
3. Personal data that is disclosed in accordance with compulsory legal process, and for which the covered organization received reimbursement of costs by the covered government entity.
4. Personal data obtained about an employee or applicant for employment, if only used for employment-related purposes.
5. Personal data that is obtained by a covered governmental entity for a background check, with the consent of the covered person.
6. Personal data (except biometric information) that is or is solely derived from lawfully obtained public data, but only if the agency receives attestations under penalty of perjury from every entity in the chain of transfers from the initial organization that collected the data until the organization selling the data to the federal agency that the personal data was obtained in compliance with all laws and regulations.

This section also requires State and local law enforcement agencies, if they use Federal funds or through interstate commerce, purchase covered personal data, to annually report the amount of money spent on such purchases; the categories of covered personal data purchases; and an estimate of the total number of covered persons whose data was purchased.

Title III—Additional reforms relating to activities under the Foreign Intelligence Surveillance Act of 1978

Sec. 301. Court supervision of collection targeting United States persons and persons located inside the United States.

This section prohibits the government from intentionally targeting any covered person for the purpose of acquiring foreign intelligence information, where such acquisition—

1. Consists of communications content, location information, web browsing history, or internet search history of the covered person; or
2. Occurs under circumstances in which the person has a reasonable expectation of privacy or a warrant would be required if a law enforcement officer sought to compel production of the information inside the United States for law enforcement purposes

unless the person is the subject of a FISA warrant or emergency authorization or criminal warrant.

This section also prohibits the government from intentionally targeting a covered person for the purpose of collecting foreign intelligence information through the installation and use of a pen register or trap and trace (PR/TT) device, or to acquire information for which a PR/TT order would be required in the United States, unless the person is the subject of a FISA order or emergency authorization or criminal PR/TT order.

This section applies regardless of the location of the acquisition. This section replaces sections 703, 704 and 705 of FISA.

Sec. 302. Consistent disclosures of relevant information in Title V and other FISA applications.

This section requires the government to certify in FISA applications that the application fairly reflects all information that calls into question any information or assessment, or otherwise raises doubts about requested findings. This is already required for applications under Title V of FISA.

Sec. 303. Strengthening accuracy procedures.

This section requires that applications to the FISA Court be accompanied by a description of procedures used by the applicant to ensure that the application is accurate and complete. The applicant must certify that they collected and reviewed:

- Supporting documentation for each factual assertion in the application
- All information that might reasonably call into question the accuracy of the information or the reasonableness of any assessment in the application or otherwise raise doubts about the findings; and
- All material that might reasonably call into question the reliability and reporting of information from a confidential human source used in the application.

The required accuracy procedures shall be adopted by the Attorney General and shall ensure that the requirements of the certification are met, that a complete file documenting each factual assertion is maintained, that the applicant coordinates with appropriate elements of the Intelligence Community concerning any relationship with the target, and that the applicant's federal agency has established annual compliance and auditing mechanism to assess the efficacy of the accuracy procedures.

These accuracy procedures are required to be created within 180 days of enactment of this Act. On the 180th day, the requirement in existing law related to narrower accuracy procedures is repealed.

Sec. 304. Clarification regarding treatment of information and evidence acquired under the Foreign Intelligence Surveillance Act of 1978.

Current law requires the government to provide notice when it intends to use evidence obtained or "derived from" FISA surveillance. This section clarifies that this requirement applies when the government would not originally have possessed the information or evidence but for FISA collection, regardless of any claim that the information or evidence is attenuated from that collection, that it would inevitably have been discovered, or was subsequently reobtained through other means.

The section requires the Attorney General and the DNI to publish policies and guidance concerning the application of this clarification.

Sec. 305. Sunset on grandfather clause of Section 215 of the USA PATRIOT Act.

On March 15, 2020, Congress allowed Section 215 of the USA PATRIOT Act, the so-called "business records provision," to expire. Existing law includes a grandfather clause allowing the continued use of Section 215 for foreign intelligence investigations that began before March 15, 2020, or for any offenses or potential offenses that began or occurred before March 15, 2020. This section sunsets this continued use of Section 215 of USA PATRIOT Act, now roughly six years after its expiration, by ending the grandfather clause after 180 days of GSRA's enactment.

Sec. 306. Written record of Department of Justice interactions with Foreign Intelligence Surveillance Court.

This section requires that the Attorney General maintain all written communications with the FISA Court and document a summary of oral communications with the Court, including the identities of the employees of the court involved in the communication, regarding an application or order.

Sec. 307. Appointment of amici curiae and access to information.

This section is based on the 2020 Lee-Leahy amendment to the USA FREEDOM Reauthorization Act, which passed the Senate 77-19. It expands the role of the FISC amici, by requiring the amici to assist the FISA Court in additional scenarios that threaten Americans' rights, by providing the amici with access to the classified case law of the FISA Court, and by permitting the amici to collaborate and raise concerns independently with the FISA Court, regardless of whether the court requested their involvement in a particular matter.

Sec. 308. Declassification of significant decisions, orders, and opinions.

This section expands the FISA Court orders subject to declassification review to include any novel or significant construction or interpretation of any term and any decision, order or opinion nominated for review by an amicus curiae appointed by the Court. The section requires the completion of the declassification review within 180 days of issuance by the Court.

Sec. 309. Clarification of Foreign Intelligence Surveillance Court jurisdiction Over records of the court and other ancillary matters.

This section provides that the FISA Court and Court of Review have jurisdiction to hear any claims ancillary to their own proceedings, including jurisdiction to hear any claim for access to the Court's records, files and proceedings. A party may file a petition for review of the FISA Court's determination related to the claim with the FISA Court of Review, and a writ of certiorari to the Supreme Court for review of a determination by the FISA Court of Review.

Sec. 310. Grounds for determining injury in fact in civil actions relating to surveillance under the Foreign Intelligence Surveillance Act of 1978 or pursuant to executive authority.

This section provides that a U.S. person or person inside the United States making a claim in a civil action relating to the acquisition, copying, querying, retention, access or use of information acquired under FISA or other authority has suffered an injury in fact if the person regularly communicates foreign intelligence information with non-U.S. persons outside the United States and has taken objectively reasonable steps to avoid surveillance; or if the person has a reasonable basis to believe that their rights have been, are being, or imminently will be violated.

The section applies the procedures of 50 U.S.C. 1806(f) (in camera, ex parte review) after any state secrets assertion, if a plaintiff plausibly alleges an injury-in-fact related to surveillance and plausibly alleges that the surveillance violates the Constitution or laws of the United States.

Sec. 311. Accountability procedures for violations by Federal employees.

This section requires the FBI, CIA, NSA and ODNI to establish procedures for accountability for individuals who commit negligent, reckless, willful or knowing violations of FISA or Executive Order 12333 if the violations result in the inappropriate collection, use, querying or dissemination of the communications, records, or information of a U.S. person or person inside the United States. The procedures include tracking and escalating consequences for such violations. These procedures supersede the more limited requirements already in law.

The provision requires reporting to Congress on the procedures and actions taken pursuant to the procedures.

Sec. 312. Reforms to the exclusive means limitations under the Foreign Intelligence Surveillance Act of 1978.

This section specifies that the provisions of the Electronic Communications Privacy Act and the Foreign Intelligence Surveillance Act are the exclusive means for the interception of wire, oral, and electronic communications:

- within the United States;
- from a domestic electronic communications system; or
- for which the sender and all intended recipients are located within the United States.

This section specifies that the Foreign Intelligence Surveillance Act and Title IV of the Government Surveillance Reform Act are the exclusive means by which the government, for foreign intelligence purposes, may acquire location information of persons in the United States.

Title IV—Reforms related to surveillance conducted for foreign intelligence purposes other than under the Foreign Intelligence Surveillance Act of 1978.

Sec. 401. Definitions.

This section defines for this title, terms consistent with their definitions in the National Security Act and the Foreign Intelligence Surveillance Act.

Sec. 402. Protections related to warrantless queries for the communications of United States persons and persons located in the United States.

This section provides the same protections for covered persons for information acquired outside FISA, to those that Section 101 of this bill provides for information acquired under FISA section 702

This section defines “query” to mean the use of any terms to retrieve any information acquired for foreign intelligence purposes, other than under FISA, whether manually or by automated means.

This section defines “covered query” to mean a query using a term associated with a covered person or to retrieve information of or concerning covered persons.
using a term associated with a covered person or with a significant purpose to access information of or concerning covered persons.

This section defines “covered information” to mean communications content; and other information, the compelled disclosure of which requires a probable cause warrant if sought for law enforcement purposes in the United States.

Warrant to access Americans’ communications and other covered information: This section requires the government to obtain a warrant, FISA court order, or FISA emergency authorization before accessing covered information returned in response to a covered query, with exceptions for:

- Exigent circumstances, with notification to the FISA Court and Congress (the official accessing the information 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 (for example, if the subject of a search is a potential victim or target of a foreign plot)
- Defensive cybersecurity purposes, with notification to the FISA Court and Congress

This prohibition does not prevent the government from conducting queries without accessing a covered persons' warrant-protected information, or from accessing communications metadata.

Foreign intelligence purpose required: This section requires a foreign intelligence purpose for all queries, including queries for metadata, unless the existing exceptions that permit the FBI to make evidence-of-a-crime queries for 702-acquired information apply. These are:

- Emergency queries, where there is "reasonable belief that such query may retrieve information that could assist in mitigating or eliminating a threat to life or serious bodily harm"
- Preservation or production obligations in litigation, and discovery obligations in criminal matters

Documentation of accesses of covered information: This section requires that all accesses of covered information in response to a covered query are documented in an electronic record system that records:

- The date of the access
- The identifier of the officer/employee who did the particular access
    - For automated accesses, this is the officer or employee who was the proximate cause of such access
- A statement of facts showing that the access was authorized by a warrant or FISA court order/emergency authorization, or an exception

Documentation of queries: This section requires that all queries are documented in an electronic record system that records:

- Each term used for the query
- The date of the query
- The identifier of the officer/employee who conducted the query
    - For automated queries, this is the officer or employee who was the proximate cause of such query
- A statement of facts justifying the query would retrieve foreign intelligence information, or the basis for an exception

Sec. 403. Prohibition on reverse targeting of United States persons and persons located in the United States.

This section provides the same protections against “reverse targeting” for intelligence activities outside of FISA, to those that Section 103 of this bill provides for targeting under FISA section 702.

This section prohibits the intentional targeting of a non-U.S. person located outside the United States, if a significant purpose is to acquire the information of a particular, known covered person, with exceptions for:

- Exigent circumstances (if there is a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm to such covered person)
- Consent

Sec. 404. Prohibition on intelligence acquisition of United States person data.

This section creates a general prohibition on elements of the intelligence community acquiring datasets containing information about covered persons using non-statutory authorities. It includes common-sense exceptions for:

- Warrants or FISA court orders or emergency authorizations
- Employment-related purposes
- Compliance with statutes, guidelines, procedures, or the Constitution
- Exigent circumstances (if there is a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm)
- Consent
- Datasets with data concerning covered persons that is not segregable, if the government exhausts all reasonable means to exclude such data prior to operational use
- Data that the government could compel with a national security letter, provided that the acquisition occurs through noncompulsory means outside the United States, compelled production is not feasible, and the acquisition is consistent with all limitations and recordkeeping required under its national security authorities

The 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 U.S. persons and persons in the United States that is significant in volume, proportion, or sensitivity. This report is also required to include the number of covered persons affected by any violations of this section, as well as any changes to minimization procedures to address compliance issues. The DNI shall also notify Congress of changes to the information in the report. Unclassified versions of the report and notifications shall be public.

Sec. 405. Prohibitions on the warrantless acquisition of domestic communications.

This section provides protections for warrantless surveillance of communications outside FISA, similar to those that section 106 of this bill creates for collection under section 702 of FISA. This section prohibits the government from intentionally acquiring for foreign intelligence purposes any communication as to which the sender and all intended recipients are known to be located in the United States, except:

- As authorized by Titles I or III of FISA; and
- Exigent circumstances (if there is a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm)

Sec. 406. Data Retention Limits

This section creates analogous data retention limitations for collection outside FISA, to those that section 104 of this bill creates for collection under section 702 of FISA.

This section requires that the Attorney General develop and entities of the intelligence community implement procedures for destroying within five years of collection, for information acquired outside FISA:

3. Any information or communication pertaining to a covered person, including an encrypted communication to or from a covered person, that has been evaluated and is not specifically known to contain foreign intelligence information; and
4. Any unevaluated information, unless it can reasonably be determined that it does not contain information pertaining to a covered person or any encrypted communication to or from a covered person.

Information need not be destroyed if the Attorney General determines in writing that:

3. The information is the subject of a preservation obligation in litigation, in which case it must be used solely for that purpose and destroyed after it is no longer required to be preserved; or
4. The information is being used in a proceeding or investigation consistent with section 706(a) of FISA (as amended by Section 102 of this bill).

Sec. 407. Reports on Violations of Law or Executive Order

Current law requires the DNI to submit to the congressional intelligence committees an annual report on violations of law or executive order committed by Intelligence Community personnel, including violations referred to the Department of Justice for possible criminal prosecution and violations substantiated by an Intelligence Community Inspector General. This section.requires that the report be made public with redactions necessary to protect sources and methods.

The section also requires that a version of the report covering violations of FISA be submitted to the congressional judiciary committees.

Title V—Independent Oversight

Sec. 501. Inspector General Oversight of Orders Under the Foreign Intelligence Surveillance Act of 1978.

This section requires the Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community to conduct an audit of applications for

court orders made, and section 702 directives issued, by the Department or the element, respectively.

The section requires that the IG review a random sampling of applications and directives and assess whether:

1. adequate safeguards are in place to ensure that the assertions made in each application are scrupulously accurate.
2. adequate safeguards are in place to ensure that each application includes all information required to be included by amendments in the 2024 Reforming Intelligence and Securing America Act and this Act.
3. The information provided by the Department of Justice meets accuracy and completeness standards.

Sec. 502. Intelligence Community Parity and Communications with Privacy and Civil Liberties Oversight Board.

This section provides that whistleblowers who lawfully disclose information to the Privacy and Civil Liberties Oversight Board are protected from reprisals.

The section changes the maximum pay for PCLOB staff, so that it is the same as the highest amount paid by any IC element for a comparable position, based on salary information provided to the Board chair by the DNI.

Sec. 503. Congressional Oversight of Grants of Immunity by the Attorney General for Warrantless Surveillance Assistance.

Current federal law allows the Attorney General to grant civil immunity to a third party for surveillance assistance not ordered by a court. This section requires Congressional notification within 30 days for any grants of immunity by the Attorney General.

Title VI—Reforms to the Electronic Communications Privacy Act of 1986

Sec. 601. Warrant protections for location information, web browsing records, and search query records.

This section requires Federal law enforcement to obtain a warrant to obtain location information (whether through compulsion or other means), or to compel online service providers into turning over historical web browsing records or search query records, which include instructions to and answers from AI assistants like Alexa and Siri. This section also requires law enforcement agencies to obtain a warrant to compel the prospective disclosure of web browsing records.

Sec. 602. Consistent protections for phone and app-based call and texting records.

This section harmonizes differing rules for Federal law enforcement access to records about phone calls and text messages. Under existing federal law, law enforcement can obtain records from phone companies with a subpoena, but from app companies only with a court order.

Sec. 603. Email Privacy Act.

This section updates the Electronic Communications Privacy Act to require Federal law enforcement agencies to obtain a warrant in order to obtain emails and other stored communications. The warrant requirement does not apply to (1) communications obtained from a service provider if they are corporate communications by their own employees; and (2) online advertisements that are readily available to the general public. This section preserves Congressional authority to obtain information from online service providers.

Sec. 604. Consistent protections for demands for data held by interactive computing services.

This section requires Federal law enforcement to follow the same procedures currently required for obtaining data from providers of electronic communication service or remote computing service when obtaining data held by interactive computing services (that is, the websites and apps that Americans use every day).

Sec. 605. Consistent protections for real-time and historical communications metadata.

This section modifies the showing required for Federal law enforcement to obtain real-time communications metadata (such as records showing when an email was sent, by whom, and to whom) to be consistent with the standard required under the Stored Communications Act for historical metadata. Currently, to compel historical metadata, the government must demonstrate to a judge specific and articulable facts showing that there are reasonable grounds to believe that the records sought are relevant and material to an ongoing criminal investigation. In contrast, to obtain the same records in real-time, law enforcement agencies must only certify to the court that the information likely to be obtained is relevant to an ongoing criminal investigation.

Sec. 606. Subpoenas for certain subscriber information.

This section prohibits Federal law enforcement from obtaining subscriber or customer information for unknown targets with just a subpoena, by requiring law enforcement to provide the name, address or an account identifier for the subscriber or customer. Existing law permits law enforcement agencies to obtain such information from an electronic communication service provider or remote computing service provider without providing any identifying information. Existing law therefore permits law enforcement to request subscriber or customer information in bulk, for example, based on browsing history or search engine records.

Sec. 607. Minimization standards for voluntary disclosure of customer communications or records.

This section requires the Attorney General to issue and publicly make available minimization procedures for certain voluntary disclosures by providers of electronic communication service and remote computing service providers to the public to Federal agencies. These voluntary disclosures are authorized when a disclosure is necessarily incident to the rendition of a service or to the protection of the rights or property of the service, or when the service provider makes an emergency disclosure.

Sec. 608. Consistent privacy protections for data held by data brokers.

This section provides that Federal law enforcement cannot compel data from covered organizations that are not online service providers (such as data brokers) without obtaining an order on the same basis and subject to the same limitations for an order to demand data from an online service provider.

Sec. 609. Protection of data entrusted to intermediary or ancillary service providers.

This section defines an intermediary or ancillary service provider as an entity or facilities owner or operator that directly or indirectly delivers, transmits, stores or processes communications or any other covered personal data for or on behalf of an online service provider. This definition extends privacy protections to data held by the many Internet intermediaries that handle Americans' communications, even though Americans do not directly interact with those providers.

This section extends the protections of the Electronic Communications Privacy Act, which currently apply to user communications and metadata held by electronic communications service providers (such as email providers and cell phone companies) to intermediary and ancillary service providers.

Sec. 610. Modernizing Criminal Surveillance Reports.

This section adds to the annual wiretap report published by the Administrative Office of the United States Courts aggregated reporting for surveillance of stored records and communications content under the Stored Communications Act and the interception of metadata under the Pen Register Act.

Sec. 611. Limitation of amendments to Federal departments and agencies.

This section clarifies that the amendments in Title VI only apply to Federal agencies, and do not affect the authorities to state and local agencies. It also provides that, if state and local agencies obtain any records in a manner that would violate Federal law if acquired by a Federal agency,

that a Federal agency may not acquire those records directly from state and local agencies or use those records as evidence in investigations or proceedings.

Title VII—Protection of Car Data from Federal Warrantless Searches

Sec. 701. Protection of car data from Federal warrantless searches.

This section requires Federal law enforcement officers to obtain a search warrant to obtain vehicle data, whether stored in the vehicle or in the cloud. There is an exception for emergencies and with the consent of the vehicle operator, as long as no passenger over the age of 14 objects.

The warrant requirement does not apply to data from event data recorders accessed by crash safety inspectors, data transmitted automatically to a 9-1-1 dispatch service, or anonymized data used for traffic safety research.

Vehicle data is defined broadly as all data processed or stored by a noncommercial vehicle, including data from diagnostic, telematics, entertainment, navigation, autonomous driving and communication systems, as well as event data recorders. It includes data using computing, storage and communication systems installed, attached to, or carried in the vehicle.

Title VIII—Intelligence Transparency

Sec. 801. Enhanced annual reports by Director of the Administrative Office of the United States Courts.

Current law requires an annual public report by the Director of the Administrative Office of the U.S. Courts. This section expands the reporting requirement to include:

1. The number of certifications by the FISA Court for the FISA Court of Review;
2. The number of petitions made by an amicus curiae for the FISA Court of Review;
3. The number of hearings or rehearings by the FISA Court en banc; and
4. The number of times amici curiae have been appointed.

Sec. 802. Enhanced annual reports by Director of National Intelligence.

This section expands the annual public reporting by the DNI to include information and data on 702 targeting; the dissemination of intelligence reports derived from both 702 and non-FISA intelligence collection that include U.S. person information; U.S. person queries of non-FISA intelligence collection, and the use in criminal proceedings of information derived from non-FISA intelligence collection.

Sec. 803. Annual reporting on accuracy and completeness of applications

This section requires annual reporting by the Attorney General on the accuracy and completeness of applications to the FISA Court.

Sec. 804. Allowing more granular aggregate reporting by recipients of foreign intelligence surveillance orders.

Under existing federal law, companies that receive FISA orders, 702 directives, and national security letters are permitted to publish statistical reports on the surveillance orders they receive for user data. Existing law permits disclosures, rounded up to the nearest 1000. This section allows companies to report data at a more fine-grained level: 0, 200, and then in bands of 200, until 1000, after which the exact number could be revealed.

Sec. 805. Report on use of foreign intelligence surveillance authorities regarding protected activities and protected classes.

This section requires the PCLOB to report publicly on the use of First Amendment-protected activities and expression, and race, ethnicity, national origin, and religious affiliation, in applications for FISA orders and in investigations for which such orders are sought.

Sec. 806. Publication of estimates regarding communications collected under certain provisions of Foreign Intelligence Surveillance Act of 1978.

This section requires that the DNI publish a good-faith estimate of:

1. The number of U.S. persons whose communications are collected under section 702; and
2. The number of communications collected under section 702 to which a party is a person located in the United States.

Sec. 807. Enhanced reporting of assessments of compliance with emergency order requirements under certain provisions of Foreign Intelligence Surveillance Act of 1978.

Current law requires that the Attorney General assess compliance with requirements for Title I emergency orders for electronic surveillance and Title III emergency orders for physical searches, This section requires that such assessment occur at least annually.

TITLE IX—Severability and Limited Delays in Implementation

Sec. 901. Rule of construction with respect to state and local law enforcement authorities.

This section clarifies that nothing in GSRA, or amendments made by GSRA, modify the authorities or affect the procedures for how a state or local department or agency can acquire records.

Sec. 902. Severability.

This section specifies that if any provision of this Act is held to be unconstitutional, the remaining provisions of the Act shall not be affected.

Sec. 903. Limited delays in implementation.

This section permits the Attorney General, in coordination with the Director of National Intelligence, to delay implementation of a provision in this Act for up to 1 year, upon a showing to the Congressional intelligence and judiciary committees, that the delay is necessary:

1. to develop and implement technical systems needed to comply with the provision or amendment; or
2. to hire or train personnel needed to comply with the provision or amendment.