Government Surveillance Reform Act

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

Sec. 101. Prohibition of Warrantless Queries for the Communications of United States Persons and Persons Located in the United States.

This section prohibits queries of information collected under Section 702 to find communications or certain information of or about U.S. persons or persons located in the United States. The information for which such queries are prohibited is that information the compelled production of which would require a probable cause warrant if sought for law enforcement purposes in the United States. Pursuant to Section 601 of the bill, such information includes geo-location information as well as web browsing and internet search history.

Queries are not prohibited:

1. When the subject of the query is the subject of an order or emergency authorization under Title I or Title III of FISA, or a criminal warrant;
2. When the individual conducting the query has 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 threat; or
3. When the subject of the query or, if such person is incapable of providing consent, a third party legally authorized to consent on behalf of that person, has provided consent to the query.

The prohibition does not apply to queries for communications metadata. However, for all queries to find information of or about U.S. persons or persons located the United States, including queries for communications metadata, the bill requires documentation of the query term, the date of the query, the identifier for the person conducting the query, and a statement of facts showing that the query was reasonably likely to retrieve foreign intelligence information or necessary to address the imminent threat of death or serious bodily harm

The results of queries to find communications metadata of or about U.S. persons or persons located in the United States may not be used as a basis for reviewing communications or information if a query for that communication or information is otherwise prohibited. However, the results of such queries may be used to identify malicious software transmitted to U.S. persons and persons located in the United States.

The section applies to federated or mixed datasets unless a mechanism exists to limit the query to information not acquired under Section 702.

Sec. 102. Limitation on Use of Information Obtained Under Section 702 Relating to United States Persons and Persons Located in the United States in criminal, civil, and administrative actions.

This section prohibits section 702-acquired information of or about, a U.S. person or person located in the U.S. from being used as part of any criminal, civil, or administrative proceeding or investigation except with the prior approval of the Attorney General and only in a proceeding or investigation in which the information is directly related to and necessary to address a specific threat of:

1. Terrorism;
2. Counterintelligence;
3. Proliferation or use of a weapon of mass destruction;
4. A cybersecurity breach or attack from a foreign country;
5. Incapacitation or destruction of critical infrastructure;
6. An attack against the armed forces or other government personnel of the U.S. or an ally;
7. International narcotics trafficking.

Sec. 103. Repeal of Authority for the Resumption of Abouts Collection.

This section repeals the authority to resume "abouts" collection under Section 702, i.e. the collection of communications that are about a target but not to or from a target. . Existing law permits the resumption of "abouts" collection, with a requirement of congressional notification..

Sec. 104. 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 acquisition if a significant purpose is to acquire the information of one or more United States persons or persons believed to be located inside the United States.

The provision includes exceptions involving an imminent threat of death or serious bodily harm; or when the person whose data is acquired provides consent.

Sec. 105. 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:

1. Any information, including an encrypted communication, to, from, or pertaining to a United States person or person reasonably believed to be located in the United States if it 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 communications to, from or pertaining to a United States person or person reasonably believed to be located in the United States.

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 where the use of the information is permitted under Section 102.

Sec. 106. 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 assistance necessary to accomplish the acquisition. 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 Court issues an order provided to the ECSP describing that technical assistance.

Sec. 107. 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 located in the United States at the time of communication.

Section 108. Requirement of a Foreign Intelligence Purpose.

Current law requires that a significant purpose of a 702 acquisition be to obtain foreign intelligence information. This section requires that obtaining foreign intelligence information be the purpose.

Sec. 109. Four-Year Extension of Section 702.

This provision extends Section 702 until September 30, 2027. This not only extends the sunset by another 4 years, but changes the date expiration from the end of December to the end of September.

Title II—Additional Reforms Relating to Activities Under the Foreign Intelligence Surveillance Act of 1978

Sec. 201. Court Supervision of Collection Targeting United States Persons and Persons Located inside the United States.

This section prohibits the government from intentionally targeting any U.S. person, regardless of location, or a person reasonably believed to be located in the United States for the purpose of acquiring foreign intelligence information 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 purpose, unless the person is the subject of a FISA warrant or emergency authorization or criminal warrant.

This section prohibits the government from intentionally targeting any U.S. person, regardless of location, or a person reasonably believed to be located in the United States for the purpose of collecting foreign intelligence information through the installation and use of a pen register or trap and trace (PRTT) device or to acquire information for which a PRTT order would be required in the United States unless the person is the subject of a FISA order or emergency authorization or criminal PRTT order.

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

Sec. 202. Required Disclosure of Relevant Information in Foreign Intelligence Surveillance Act of 1978 Applications.

This section requires the government to disclose to the Foreign Intelligence Surveillance Court all information that is material to the Court's determination, including exculpatory information, information that calls into question the accuracy of an application or the reasonableness of an assessment in an application, and information that otherwise raises doubts with respect to the findings on which a determination is made.

Sec. 203. Certification Regarding Accuracy Procedures.

This section requires that applications to the FISA Court be accompanied by a description of accuracy procedures used by the applicant and a certification that the officer making the application has 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 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.

Sec. 204. 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 obtained through other means.

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

Sec. 205. Sunset on Grandfather Clause of Section 215 of USA PATRIOT Act.

This provision sunsets a grandfather clause that allows the continued use of Section 215 of the USA PATRIOT Act 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 sunset occurs 180 days after enactment of this bill.

Sec. 206. Written Record of Department of Justice interactions With Foreign Intelligence Surveillance Court; Protections Against Judge Shopping by DOJ

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.

The section requires that, to the extent practicable, any extensions of FISA orders be granted or denied by the same judge who issued the original order.

Sec. 207. 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. 208. 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.

Sec. 209. 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. 210. 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 abrogates the state secrets privilege and applies the procedures of 50 U.S.C. 1806(f) (in camera, ex parte review), 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. 211. 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.

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

Title III—Reforms Related to Surveillance Conducted Under Executive Order 12333

Sec. 301. Definitions.

This section defined for purposes of Title III related to Executive Order 12333 terms consistent with their definitions in the National Security Act and the Foreign Intelligence Surveillance Act.

Sec. 302. Prohibition of Warrantless Queries for the Communications of United States Persons and Persons Located in the United States.

This section prohibits queries of information collected pursuant to Executive Order 12333 or successor order (but not FISA) to find communications or certain information of or about U.S. persons or persons located in the United States. The information for which such queries are prohibited is that information the compelled production of which would require a probable cause warrant if sought for law enforcement purposes in the United States. Pursuant to Section 601 of the bill, such information includes geo-location information as well as web browsing and internet search history.

Queries are not prohibited:

1. When the subject of the query is the subject of an order or emergency authorization under Title I or Title III of FISA, or a criminal warrant;
2. When the individual conducting the query has a reasonable belief that an emergency exists involving an imminent threat of death or serious bodily harm to the subject of the query and the information is sought for the purpose of preventing or mitigating the threat; or
3. When the subject of the query or, if such person is incapable of providing consent, a third party legally authorized to consent on behalf of that person, has provided consent to the query.

The prohibition does not apply to queries for communications metadata. However, for all queries to find information of or about U.S. persons or persons located the United States, including queries for communications metadata, the bill requires documentation of the query term, the date of the query, the identifier for the person conducting the query, and a statement of facts showing that the query was reasonably likely to retrieve foreign intelligence information.

The results of queries to find communications metadata of or about U.S. persons or persons located in the United States may not be used as a basis for reviewing communications or information if a query for that communication or information is otherwise prohibited. However, the results of such queries may be used to identify malicious software transmitted to U.S. persons and persons located in the United States.

Sec. 303. Prohibition on Reverse Targeting of United States Persons and Persons Located in the United States.

This section prohibits the targeting under Executive Order 12333 of any person if a significant purpose of the acquisition is to target one or more U.S. persons or persons reasonably believed to be located in the United States in violation of the targeting prohibitions in Section 201..

The provision includes an emergency exception involving an imminent threat of death or serious bodily harm; or when with the consent of the person whose data is acquired provides consent.

Sec. 304. Prohibition on Intelligence Acquisition of United States Person Data.

This section prohibits an element of the intelligence community from acquiring a dataset that includes covered data, defined as data, derived data, or any unique identifier that is linked to or is reasonably linkable to a United States person or person reasonably believed to be located in the United States.

Covered data does not include data that is:

1. Lawfully available to the public through Federal, State, or local government records or through widely distributed media;
2. Reasonably believed to have been voluntarily made available to the general public by the covered person; and
3. Related to a specific communication or transaction with a targeted individual who is not a covered person.

The section permits the acquisition if it has been authorized pursuant to an order or emergency authorization pursuant to FISA or the Federal Rules of Criminal Procedure.

The section exempts from the prohibition acquisition for employment-related purposes; for purposes of compliance with statutes, guidelines, procedures and the U.S. Constitution; to respond to an emergency involving an imminent threat of death or serious bodily harm; and 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 destroyed when it is no longer necessary for that purpose.

The section requires minimization procedures that permit the acquisition of datasets that include covered data if the government exhausts all reasonable means to exclude any non-exempted covered data prior to acquisition and then to remove and delete the non-exempted covered data prior to the operational use of the dataset or the inclusion of the dataset in a database intended for operational use. Data acquired in violation of this section shall be destroyed upon recognition and may not be used in criminal or civil actions.

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, 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. 305. Prohibitions on the Warrantless Acquisition of Domestic Communications.

This section prohibits the government from intentionally acquiring pursuant to Executive Order 12333 any communication as to which the sender and all intended recipients are known to be located in the United States, except as authorized under FISA.

The section permits the acquisition in the case of emergency involving the imminent threat of death or serious bodily harm.

Sec. 306. Data Retention Limits

This section requires that the Attorney General develop and entities of the Intelligence Community implement procedures, applicable to collection under EO 12333, for destroying within five years of collection:

3. Any information, including an encrypted communication, to, from or pertaining to a United States person or person reasonably believed to be located in the United States if it 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 communications to or from or information pertaining to a United States person or person reasonably believed to be located in the United States.

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 where the use of the information is permitted under Section 102.

Sec. 307. 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 IV—Independent Oversight

Sec. 401. 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 material information, including any information that tends to suggest that the court should deny the application or that the court should include one or more conditions in an order.r
3. The information provided by the Department of Justice meets accuracy and completeness standards.

Sec. 402. Department of Justice Inspector General Review of High Intensity Drug Trafficking Area Surveillance Programs.

This section requires the DOJ IG to conduct reviews of federally-funded surveillance programs that are operated by high intensity drug trafficking area organizations, and that provide law enforcement agencies with access to databases containing information on more than one million U.S. persons or persons in the United States.

Sec. 403. 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. 404. 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 V—Reforms to the Electronic Communications Privacy Act of 1986

Sec. 501. Warrant Protections for Location Information, Web Browsing Records, and Search Query Records.

This section requires 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. 502. Consistent Protections for Phone and App-Based Call and Texting Records.

This section harmonizes differing rules for 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. 503. Email Privacy Act.

This section updates the Electronic Communications Privacy Act to require law enforcement agencies to obtain a warrant in order to obtain emails and other stored communications. The warrant requirement does not apply to corporate communications, online advertisements, or communications compelled from a party to the communication. This section does not limit Congressional authority to obtain information from online service providers.

Sec. 504. Consistent Protections for Demands for Data Held by Interactive Computing Services.

This section requires 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. 505. Consistent Protections for Real-Time and Historical Communications Metadata.

This section modifies the showing required for 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. 506. Subpoenas for Certain Subscriber Information.

This section prohibits 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. 507. 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. 508. Prohibition on Law Enforcement Purchase of Personal Data from Data Brokers.

This section prohibits law enforcement agencies from purchasing personal data about U.S. persons and persons in the U.S.

This prohibition has 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.
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 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 that is or is derived from lawfully obtained public data.

Sec. 509. Consistent Privacy Protections for Data Held by Data Brokers.

Provides that 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. 510. 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 as well.

Sec. 511. 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.

Title VI—Regulation of government surveillance using cell site simulators, general prohibition on private, non-research use.

Sec. 601. Cell-Site Simulators.
This section creates a statutory legal framework for government agencies to use cell-site simulators (CSS) (often known as "Stingrays"). Other uses of CSS are prohibited, with a fine of up to $250,000 for unlawful use. There is also an exception to this prohibition for good-faith cybersecurity researchers and educators.

Except in emergencies, law enforcement agencies may only use CSS to conduct surveillance with a warrant. The process to obtain the warrant requires a robust review by the court to ensure that the impact of the technology on the community is minimized. Warrants may be issued for 30 days at a time, renewable. Emergency use is permitted, as long as a warrant is obtained within 48 hours of the initial use. No warrant is required to locate a lost, missing, abducted, or kidnapped person, or to find victims after a mass casualty event, and the Department of Defense is permitted to help law enforcement for such domestic search and rescue missions.

Intelligence community use is regulated as follows:

- The existing carve-out of FISA in 50 U.S.C. 1802(a)(1) that permits warrantless surveillance of foreign embassies and government-only communications systems also applies to the use of CSS.

- Other use must be pursuant to a Title I FISA court order (under 50 U.S.C. 1805).

The warrant requirement does not apply to:

- The Secret Service when protecting the President and other officials.
- Correctional facilities taking reasonable steps to limit transmissions outside their land.
- Testing and training by the government and FCC-accredited testing labs.

This section provides a cause of action for any person subject to an unlawful operation of a cell-site simulator to bring a civil suit for appropriate relief (including declaratory and injunctive relief, actual damages, statutory damages of up to $500 per violation, and attorney fees) against the person, including a governmental entity, that conducted the unlawful operation.

This section requires an annual public report by law enforcement and intelligence agencies inspectors general on the use of CSS.

Requires the FCC to initiate any proceeding within 180 days that is necessary to promulgate or modify existing regulations to implement this section.

Title VI—Protection of Car Data from Warrantless Searches

Sec. 701. Protection of Car Data from Warrantless Searches

This section requires 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 IX—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 of Executive Order 12333 collection that include U.S. person information, U.S. person queries of EO 12333 collection, and the use in criminal proceedings of information derived from EO 12333 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 IV—SEVERABILITY AND LIMITED DELAYS IN IMPLEMENTATION

Sec. 901. 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. 902. 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.