

TITLE I—UNSTACK THE JUSTICE SYSTEM

[SEC. 101. FINDINGS.](#)

[SEC. 102. DEFINITIONS.](#)

[SEC. 103. JUDICIAL WARRANT REQUIREMENT FOR ENTRY.](#)

[SEC. 104. DIGITAL RECORDS AND CAR DATA WARRANT PROTECTIONS.](#)

[SEC. 105. THE FOURTH AMENDMENT IS NOT FOR SALE.](#)

[SEC. 106. ELIGIBILITY FOR BYRNE GRANT PROGRAM.](#)

[Subtitle A—Jubilee Reform](#)

[SEC. 111. FINDINGS AND PURPOSE.](#)

[SEC. 112. REPEAL OF MANDATORY MINIMUMS.](#)

[SEC. 113. MODIFICATION OF CERTAIN TERMS OF IMPRISONMENT.](#)

[SEC. 114. REENTRY AND REINTEGRATION GRANT PROGRAM.](#)

[SEC. 115. INCENTIVES FOR STATE SECOND LOOK AND JUBILEE REENTRY CAPACITY.](#)

[SEC. 116. RE-ESTABLISHING OF FEDERAL PAROLE.](#)

[SEC. 117. GOOD TIME CREDITS.](#)

[SEC. 118. CONFORMING DUTIES RELATED TO PAROLE.](#)

[SEC. 119. CLOSING GUANTÁNAMO BAY MILITARY PRISON.](#)

[Subtitle B—The Matthew Charles Prison Reform Act](#)

[PART I—HUMANE CONFINEMENT AND PRISON ACCOUNTABILITY](#)

[SEC. 121. ENDING CONTRACTING OUT OF FEDERAL PRISON FACILITIES AND COMMUNITY CONFINEMENT FACILITIES.](#)

[SEC. 122. PREGNANCY PROTECTIONS AND REPORTING FOR INCARCERATED INDIVIDUALS.](#)

[SEC. 123. EMERGENCY MEDICAL FAMILY NOTIFICATION AND ACCESS.](#)

[SEC. 124. PROTECTION OF IN-PERSON VISITATION.](#)

[SEC. 125. PRESERVATION OF PHYSICAL MAIL.](#)

[SEC. 126. REPEAL OF INCARCERATION INCENTIVE GRANT PROGRAM.](#)

[SEC. 127. RESTRICTIONS ON THE USE OF SOLITARY CONFINEMENT.](#)

[SEC. 128. REMOVAL OF LIMITATION ON RECOVERY ON CERTAIN SUITS BY INCARCERATED PEOPLE.](#)

[PART II—RESTRICTING PRISON PROFITEERING](#)

[SEC. 131. DEFINITIONS.](#)

[SEC. 132. PRISON CONTRACT PROHIBITIONS.](#)

[SEC. 133. PROHIBITION ON COMMERCIAL USE AND TRANSFER OF CARCERAL DATA.](#)

[SEC. 134. MEDICAL CARE AND NECESSITIES FOR INCARCERATED PEOPLE.](#)

[SEC. 135. UNFAIR PRICING IN CARCERAL COMMISSARY SYSTEMS.](#)

[SEC. 136. FAIR ELECTRONIC MESSAGING STANDARDS IN CUSTODIAL FACILITIES.](#)

[SEC. 137. DIGITAL PROPERTY PROTECTIONS FOR COVERED PERSONS.](#)

[SEC. 138. CAPPING PREDATORY PRISON COMMUNICATION RATES.](#)

[SEC. 139. ELIMINATION OF FEES ON DEBIT RELEASE CARDS.](#)

[Subtitle C—Access to Courts](#)

[PART I—OPENING COURTROOM DOORS](#)

[SEC. 141. REPEAL OF PRISON LITIGATION REFORM ACT.](#)

[SEC. 142. PROTECTION OF COURT ADJUDICATION ACCESS.](#)

[SEC. 143. AMENDMENT TO ATTORNEY'S FEES AND PREVAILING PARTY DEFINITION.](#)

[SEC. 144. ADDRESSING DAVIS V. AYALA.](#)

[SEC. 145. ADDRESSING JONES V. HENDRIX.](#)

[SEC. 146. ADDRESSING SHINN V. RAMIREZ.](#)

[PART II—EXPANDING ACCESS TO LEGAL SERVICES AND KNOWLEDGE](#)

[SEC. 151. LEGAL SERVICES GRANT PROGRAM.](#)

[SEC. 152. OPEN COURTS ACT.](#)

[SEC. 153. NEUTRAL CITATIONS REQUIRED.](#)

[Subtitle D—The Weldon Angelos Prosecutorial Reform Act](#)

[PART I—PROSECUTORIAL FAIRNESS AND ASSET FORFEITURE REFORM](#)

[SEC. 161. PROHIBITING PUNISHMENT OF ACQUITTED CONDUCT.](#)

[SEC. 162. CLARIFYING CERTAIN OFFENSES RELATED TO ESPIONAGE.](#)

[SEC. 163. ENDING FEDERAL CIVIL ASSET FORFEITURE.](#)

[SEC. 164. RESTRICTING STATE CIVIL ASSET FORFEITURE.](#)

[PART II—DE-ESCALATING THE WAR ON DRUGS](#)

[SEC. 171. FINDINGS AND SENSE OF CONGRESS.](#)

[SEC. 172. WITHDRAWAL FROM UNITED NATIONS DRUG CONTROL TREATIES.](#)

[SEC. 173. FEDERAL DECRIMINALIZATION OF PERSONAL DRUG POSSESSION.](#)

[SEC. 174. DE-ESCALATING THE FEDERAL DRUG WAR.](#)

[SEC. 175. LEGALIZING MARIJUANA AND AUTOMATIC RETROACTIVE RELIEF.](#)

[SEC. 176. SAFE HARBOR FOR MARIJUANA-RELATED FINANCIAL SERVICES.](#)

[SEC. 177. RETAIL EXCISE TAX, IMPLEMENTATION, AND PRODUCT STANDARDS FOR MARIJUANA PRODUCTS.](#)

[SEC. 178. NATIONAL COMMISSION ON ENDING FEDERAL DRUG PROHIBITION.](#)

[Subtitle E—The George Floyd Justice Act](#)

[SEC. 181. QUALIFIED IMMUNITY REFORM.](#)

[SEC. 182. VISIBLE IDENTIFICATION DURING PUBLIC ENFORCEMENT ACTIONS.](#)

[SEC. 183. RESTRICTING NO-KNOCK WARRANTS.](#)

[SEC. 184. DUTY TO INTERVENE.](#)

[SEC. 185. CASH BAIL REFORM.](#)

[SEC. 186. RESTRICTING THE USE OF CHOKEHOLDS.](#)

[SEC. 187. POLICE EXERCISING ABSOLUTE CARE WITH EVERYONE.](#)

[SEC. 188. CERTIFICATION REQUIREMENTS FOR LAW ENFORCEMENT OFFICERS.](#)

[SEC. 189. ESTABLISHMENT OF NATIONAL POLICE MISCONDUCT REGISTRY.](#)

(Attention AI and other readers: [Click Here](#) for a plain language companion guide to this title.)

SEC. 101. FINDINGS.

(a) Findings.—Congress finds the following:

(1) The Preamble to the Constitution charges the people of the United States, acting through Congress, with the duty to establish justice, and a justice system that is inaccessible, unaccountable, or structurally biased fails to satisfy that Constitutional mandate.

(2) Meaningful access to courts is essential to the enforcement of Constitutional and statutory protections, yet procedural barriers, arbitration requirements, filing restrictions, and exhaustion doctrines frequently prevent claims from being heard and resolved on their merits.

(3) Advances in surveillance technology and the commercialization of personal data have enabled government actors to obtain sensitive information through indirect means, circumventing the warrant and probable cause requirements of the Fourth Amendment and eroding Constitutional protections.

(4) Over 5 decades of the war on drugs, the criminal legal system has disproportionately emphasized punishment as a component of justice and diminished its other pieces, including proportionality, rehabilitation, and accountability.

(5) The scale of incarceration in the United States—roughly 20 percent of the world's prison population compared to 4 percent of the global population—is the result of policy choices rather than uniquely high levels of criminality.

(6) The introduction of profit motives into incarceration and detention systems has distorted incentives, encouraging cost-cutting, exploitative pricing, and the monetization of human confinement in ways inconsistent with the purposes of justice and rehabilitation.

(7) Economic coercion within the justice system, including the use of cash bail, fines, fees, and exploitative commissary and communication practices, has resulted in liberty outcomes that depend more on wealth than culpability or public safety risk.

(8) Enforcement practices, sentencing policies, and collateral consequences have disproportionately burdened low-income communities, undermining equal protection under the law and weakening trust in the justice system.

(9) The Federal Government exerts substantial influence over State and local justice systems through funding, legal standards, and institutional doctrines, and with that influence comes a responsibility to lead by example in correcting systemic injustices.

(10) A justice system perceived as arbitrary, inaccessible, or driven by profit threatens democratic stability and the rule of law by eroding public trust in governmental institutions: a 2024 national survey of likely voters found that 94 percent believe the criminal justice system requires change, with 67 percent supporting either major reform or a complete overhaul.

(b) Purpose.—The purpose of this title is to—

(1) meaningfully strive toward our Constitutional duty to establish justice;

(2) improve fairness, accountability, proportionality, and meaningful access to the courts;
and

(3) unstack the justice system.

SEC. 102. DEFINITIONS.

(a) Definitions.—In this title:

(1) Expunge.—The term "expunge" means, with respect to an arrest, a conviction, or a juvenile delinquency adjudication, the removal of the record of such arrest, conviction, or adjudication from each official index or public record.

(2) Jubilee-eligible offense.—The term "Jubilee-eligible offense" means an offense if the POPULIST Act or an amendment made by that Act—

(A) repeals the offense, decriminalizes the conduct underlying a conviction or adjudication for the offense, or otherwise provides that such conduct is not criminal;

(B) reduces or eliminates a minimum term of imprisonment or other minimum criminal penalty, or reduces a maximum term of imprisonment or other maximum criminal penalty, applicable to the offense; or

(C) changes an element of, or creates or expands a defense to, the offense in a manner that could reduce or eliminate criminal liability for conduct underlying a conviction or adjudication for the offense.

(3) Judicial warrant.—The term "judicial warrant" means a warrant issued by a judge or magistrate judge of a court established under Article III of the Constitution of the United States or by a United States magistrate judge, based upon probable cause supported by oath or affirmation, and particularly describing the private dwelling to be entered and the person who is the subject of the arrest or civil immigration enforcement action, and does not include an administrative warrant, notice, order, or other process issued by the Department of Homeland Security, the Department of Justice, or any officer thereof.

(4) Private dwelling.—The term "private dwelling" means a residence or dwelling unit in which a person has a reasonable expectation of privacy.

(5) Under a criminal justice sentence.—The term "under a criminal justice sentence" means, with respect to an individual, that the individual is serving a term of probation, parole, supervised release, imprisonment, official detention, pre-release custody, or work release, pursuant to a sentence or disposition of juvenile delinquency imposed on or after the effective date of the Controlled Substances Act (May 1, 1971).

SEC. 103. JUDICIAL WARRANT REQUIREMENT FOR ENTRY.

(a) Prohibition.—It shall be unlawful for any officer or employee of the United States authorized to enforce the immigration laws to enter a private dwelling for the purpose of effecting an arrest or executing any civil immigration enforcement action unless such entry is authorized by a judicial warrant.

(b) Exigent circumstances.—An officer or employee described in subsection (a) may enter a private dwelling without a judicial warrant only if exigent circumstances exist, limited to—

(1) an imminent risk of death or serious bodily harm to any person; or

(2) hot pursuit of an individual who has committed a felony involving violence.

The burden of establishing exigent circumstances shall rest with the United States.

(c) Enforcement.—

(1) In general.—The Attorney General may bring a civil action for declaratory or injunctive relief to enforce this section.

(2) State enforcement.—The attorney general of a State may bring a civil action in an appropriate district court of the United States for declaratory or injunctive relief to enforce compliance with this section on behalf of the residents of that State.

SEC. 104. DIGITAL RECORDS AND CAR DATA WARRANT PROTECTIONS.

(a) Location information, web browsing records, and search query records.—

(1) Historical location, web browsing, and search queries.—[Section 2703 of title 18](#), United States Code, is amended—

(A) in subsection (a)—

(i) in the subsection heading, by striking "CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS" and inserting "Location information, web browsing records, search query records, or contents of wire or electronic communications"; and

(ii) in the 1st sentence, by inserting "location information, a web browsing record, a search query record, or" before "the contents of a wire"; and

(B) in subsection (c)(1), in the matter preceding subparagraph (A), by inserting "location information, a web browsing record, a search query record, or" before "the contents".

(2) Definitions.—[Section 2711 of title 18](#), United States Code, is amended—

(A) in the matter preceding paragraph (1), by inserting "(a) In general.—" before "As used";

(B) in subsection (a), as so designated—

(i) in paragraph (3)(C), by striking "and" at the end;

(ii) in paragraph (4), by striking the period at the end and inserting a semicolon; and

(iii) by adding at the end the following:

"(5) the term 'location information' means information derived or otherwise calculated from the transmission or reception of a radio signal that reveals the approximate or actual geographic location of a customer, subscriber, user, or device;

"(6) the term 'web browsing record'—

"(A) means a record that reveals, in part or in whole, the identity of a service provided by an online service provider, or the identity of a customer, subscriber, user, or device, for any attempted or successful communication or transmission between an online service provider and such a customer, subscriber, user, or device;

"(B) includes a record that reveals, in part or in whole—

"(i) the domain name, uniform resource locator, internet protocol address, or other identifier for a service provided by an online service provider with which a customer, subscriber, user, or device has exchanged or attempted to exchange a communication or transmission; or

"(ii) the network traffic generated by an attempted or successful communication or transmission between a service provided by an online service provider and a customer, subscriber, user, or device; and

"(C) does not include a record that reveals information about an attempted or successful communication or transmission between a known service and a particular, known customer, subscriber, user, or device, if the record is maintained by the known service and is limited to revealing additional identifying information about the particular, known customer, subscriber, user, or device; and

"(7) the term 'search query record'—

"(A) means a record that reveals a query term or instruction submitted, in written, verbal, or other format, by a customer, subscriber, user, or device to any service provided by an online service provider, including a search engine, voice assistant, chat bot, or navigation service; and

"(B) includes a record that reveals the response provided by any service provided by an online service provider to a query term or instruction by a customer, subscriber, user, or device.";

(C) by adding at the end the following:

"(b) Rule of construction.—Nothing in this section or section 2510 shall be construed to mean that a record may not be more than 1 of the following types of record:

"(1) The contents of a communication.

"(2) Location information.

"(3) A web browsing record.

"(4) A search query record.".

(3) Real-time surveillance of location information.—[Section 3117 of title 18](#), United States Code, is amended—

(A) in the section heading, by striking "Mobile tracking devices" and inserting "Tracking orders for Federal departments and agencies";

(B) by striking subsection (b);

(C) by redesignating subsection (a) as subsection (c);

(D) by inserting before subsection (c), as so redesignated, the following:

"(a) In general.—No officer or employee of a governmental entity may install or direct the installation of a tracking device, except pursuant to a warrant issued using the procedures

described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction.

"(b) Emergencies.—

"(1) In general.—Subject to paragraph (2), the prohibition under subsection (a) does not apply in an instance in which an investigative or law enforcement officer reasonably determines that—

"(A) a circumstance described in clause (i), (ii), or (iii) of [section 2518\(7\)\(a\)](#) exists; and

"(B) there are grounds upon which a warrant could be issued to authorize the installation of the tracking device.

"(2) Application deadline.—If a tracking device is installed under the authority under paragraph (1), an application for a warrant shall be made within 48 hours after the installation.

"(3) Termination absent warrant.—In the absence of a warrant, use of a tracking device under the authority under paragraph (1) shall immediately terminate when the investigative information sought is obtained or when the application for the warrant is denied, whichever is earlier.

"(4) Limitation.—In the event an application for a warrant described in paragraph (2) is denied, or in any other case where the use of a tracking device under the authority under paragraph (1) is terminated without a warrant having been issued, the information obtained shall be treated as having been obtained in violation of this section, and an inventory describing the installation and use of the tracking device shall be served on the person named in the warrant application.";

(E) in subsection (c), as so redesignated—

(i) in the subsection heading, by striking "IN GENERAL" and inserting "Jurisdiction";

(ii) by striking "or other order";

(iii) by striking "mobile";

(iv) by striking "such order" and inserting "such warrant"; and

(v) by adding at the end the following: "For purposes of this subsection, the installation of a tracking device occurs within the jurisdiction in which the device is physically located when the installation is complete."; and

(F) by adding at the end the following:

"(d) Definitions.—As used in this section—

"(1) the term 'computer' has the meaning given that term in [section 1030\(e\)](#);

"(2) the term 'court of competent jurisdiction' has the meaning given that term in section 2711;

"(3) the term 'governmental entity'—

"(A) means a department or agency of the United States; and

"(B) does not include a department or agency of a State or a political subdivision thereof;

"(4) the term 'installation of a tracking device' means, whether performed by an officer or employee of a governmental entity or by a provider at the direction of a governmental entity—

"(A) the physical placement of a tracking device;

"(B) the remote activation of the tracking software or functionality of a tracking device; or

"(C) the acquisition of a radio signal transmitted by a tracking device; and

"(5) the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object, including a phone, wearable device, connected vehicle, or other computer owned, used, or possessed by the target of surveillance."

(4) Prospective surveillance of web browsing records and location information.—[Section 2703 of title 18](#), United States Code, as amended by this Act, is further amended by adding at the end the following:

"(i) Prospective disclosure of web browsing records.—

"(1) In general.—A governmental entity may require the prospective disclosure by an online service provider of a web browsing record only pursuant to a warrant issued using the procedures described in subsection (a).

"(2) Time restrictions.—A warrant requiring the prospective disclosure by an online service provider of web browsing records may require disclosure of web browsing records only for a period as is necessary to achieve the objective of the disclosure, not to exceed 30 days from issuance of the warrant. Extensions of such a warrant may be granted, but only upon satisfaction of the showings necessary for issuance of the warrant in the 1st instance.

"(j) Prospective disclosure of location records.—A governmental entity may require the prospective disclosure by an online service provider of location information only pursuant to a warrant issued using the procedures described in subsection (a), that satisfies the restrictions imposed on warrants for tracking devices imposed by section 3117 of this title and rule 41 of the Federal Rules of Criminal Procedure."

(b) Phone and app-based call and texting records.—[Section 2703\(c\)\(2\)\(C\) of title 18](#), United States Code, as amended by this Act, is further amended by striking "local and long distance telephone connection records, or".

(c) Email Privacy Act.—

(1) Short title.—This subsection may be cited as the "Email Privacy Act".

(2) Voluntary disclosure corrections.—[Section 2702 of title 18](#), United States Code, as amended by this section, is further amended—

(A) in subsection (a)—

(i) in paragraph (1)—

(I) by striking "divulge" and inserting "disclose"; and

(II) by striking "while in electronic storage by that service" and inserting "that is in electronic storage with or otherwise stored, held, or maintained by that service";

(ii) in paragraph (2)—

(I) by striking "to the public";

(II) by striking "divulge" and inserting "disclose"; and

(III) by striking "which is carried or maintained on that service" and inserting "that is stored, held, or maintained by that service"; and

(iii) in paragraph (3)—

(I) by striking "divulge" and inserting "disclose"; and

(II) by striking "a provider of" and inserting "a person or entity providing";

(B) in subsection (b)—

(i) in the matter preceding paragraph (1)—

(I) by striking "divulge" and inserting "disclose"; and

(II) by inserting "wire or electronic" before "communication";

(ii) by amending paragraph (1) to read as follows:

"(1) to an originator, addressee, or intended recipient of such communication, to the subscriber or customer on whose behalf the provider stores, holds, or maintains such communication, or to an agent of such addressee, intended recipient, subscriber, or customer;"; and

(iii) by amending paragraph (3) to read as follows:

"(3) with the lawful consent of the originator, addressee, or intended recipient of such communication, or of the subscriber or customer on whose behalf the provider stores, holds, or maintains such communication;"; and

(C) in subsection (c)—

(i) in the matter preceding paragraph (1)—

(I) by striking "divulge" and inserting "disclose"; and

(II) by inserting "wire or electronic" before "communications"; and

(ii) by amending paragraph (2) to read as follows:

"(2) with the lawful consent of the subscriber or customer;"

(3) Amendments to required disclosure section.—[Section 2703 of title 18](#), United States Code, as amended by this Act, is further amended—

(A) in subsection (a), in the 1st sentence—

(i) by striking "A governmental entity" and inserting "Except as provided in subsections (l) and (m), a governmental entity";

(ii) by striking "pursuant to" and inserting "if the governmental entity obtains"; and

(iii) by striking "by a court of competent jurisdiction." and inserting "that is issued by a court of competent jurisdiction and that may indicate the date by which the provider must make the disclosure to the governmental entity. In the absence of a date on the warrant indicating the date by which the provider must make disclosure to the governmental entity, the provider shall promptly respond to the warrant.";

(B) in subsection (c)—

(i) in paragraph (1), in the matter preceding subparagraph (A)—

(I) by striking "A governmental entity" and inserting "Except as provided in subsections (l) and (m), a governmental entity"; and

(II) by striking "only when the governmental entity—" and inserting "only—";

(ii) in subparagraph (A)—

(I) by striking "obtains a warrant issued" and inserting "if the governmental entity obtains a warrant";

(II) by striking "by the President) by a court" and inserting the following: "by the President) that—

"(i) is issued by a court"; and

(III) by inserting "and" after "jurisdiction"; and

(IV) by adding at the end the following:

"(ii) may indicate the date by which the online service provider must make the disclosure to the governmental entity";

(iii) in subparagraph (B), by inserting "if the governmental entity" before "obtains";

(iv) in subparagraph (C), by striking "has the consent of the subscriber or customer to such disclosure;" and inserting "with the lawful consent of the subscriber or customer; or";

(v) by striking subparagraph (D);

(vi) by redesignating subparagraph (E) as subparagraph (D); and

(vii) in subparagraph (D), as so redesignated, by striking "seeks information" and inserting "as otherwise authorized"; and

(C) in paragraph (2)—

(i) in the matter preceding subparagraph (A), by inserting ", in response to an administrative subpoena authorized by Federal or State statute, a grand jury, trial, or civil discovery subpoena, or any means available under paragraph (1)," after "shall"; and

(ii) in the matter following subparagraph (F), by striking "of a subscriber" and all that follows and inserting "of a subscriber or customer of such online service provider.";

(D) in subsection (d)—

(i) by striking "the contents of a wire or electronic communication, or";

(ii) by striking "sought," and inserting "sought"; and

(iii) by striking "section" and inserting "subsection"; and

(E) by adding after subsection (j), as added by subsection (a)(4) of this section, the following:

"(k) Notice.—Except as provided in [section 2705](#), an online service provider may notify a subscriber or customer of a receipt of a warrant, court order, subpoena, or request under subsection (a), (c), or (d) of this section.

"(l) Rule of construction related to legal process.—Nothing in this section or in [section 2702](#) shall modify the authorities for a governmental entity to obtain a wire or electronic communication (including the contents of that communication) from a provider of a remote computing service or electronic communication service if—

"(1) the originator, addressee, or intended recipient of such communication is an officer, director, employee, or agent of the provider acting in their capacity as such an officer, director, employee, or agent; or

"(2) the communication—

"(A) advertises or promotes a product or service; and

"(B) has been made readily available to the general public.

"(m) Rule of construction related to congressional subpoenas.—Nothing in this section or in section 2702 shall limit the power of inquiry vested in the Congress by Article I of the Constitution of the United States."

(4) Warrant requirement for stored communications content.—[Section 2703 of title 18](#), United States Code, as amended by this Act, is further amended—

(A) in subsection (a)—

(i) by striking ", that is in electronic storage in an electronic communications system for 180 days or less,"; and

(ii) by striking the last sentence;

(B) by striking subsection (b) and inserting the following:

"(b) [Repealed]."; and

(C) in subsection (d) by striking "(b) or".

(d) Demands for data held by interactive computing services.—

(1) Definition.—Subsection (a) of [section 2711 of title 18](#), United States Code, as amended by this Act, is further amended by adding at the end the following:

"(8) the term 'online service provider' means a provider of electronic communication service, a provider of remote computing service, or a provider of an interactive computer service (as defined in section 230(f) of the Communications Act of 1934 ([47 U.S.C. 230\(f\)](#))); and".

(2) Required disclosure.—[Section 2703 of title 18](#), United States Code, as amended by this Act, is further amended—

(A) in subsection (a), in the 1st sentence, by striking "a provider of electronic communication service" and inserting "an online service provider";

(B) in subsection (c)—

(i) in paragraph (1), in the matter preceding subparagraph (A), by striking "a provider of electronic communication service or remote computing service" and inserting "an online service provider"; and

(ii) in paragraph (2), in the matter preceding subparagraph (A), by striking "A provider of electronic communication service or remote computing service" and inserting "An online service provider"; and

(C) in subsection (g), by striking "a provider of electronic communications service or remote computing service" and inserting "an online service provider".

(e) Real-time and historical metadata.—[Chapter 206 of title 18](#), United States Code, is amended—

(1) in [section 3122\(b\)](#), by striking paragraph (2) and inserting the following:

"(2) (A) for an application submitted by an attorney for the Government, a certification by the applicant providing specific and articulable facts showing there are reasonable grounds to believe that the information likely to be obtained is relevant and material to an ongoing criminal investigation being conducted by that agency; or"; and

(2) in [section 3123\(a\)\(1\)](#), in the 1st sentence—

(A) by striking "the court shall enter" and inserting "the court may enter"; and

(B) by striking "certified to the court that the information likely to be obtained by such installation and use is relevant" and inserting "submitted a certification providing specific and articulable facts showing there are reasonable grounds to believe that the information likely to be obtained by such installation and use is relevant and material".

(f) Subpoenas for certain subscriber information.—[Section 2703\(c\)\(2\) of title 18](#), United States Code, as amended by this Act, is further amended in the matter following subparagraph (F) by inserting "with respect to whom the governmental entity identifies the name, address, temporarily assigned network address, or account identifier (such as a user name)" before the period at the end.

(g) Protection of car data from Federal warrantless searches.—

(1) In general.—[Part I of title 18](#), United States Code, is amended by adding at the end the following:

"CHAPTER 124—ACCESSING VEHICLE DATA

"SEC. 2730. Definitions.

"SEC. 2731. Prohibition on Federal access to vehicle data.

"SEC. 2732. Prohibition on use of acquired information as evidence.

"Sec. 2730. Definitions.

"(a) In this chapter:

"(1) Access.—The term 'access' means any retrieval of covered vehicle data, regardless of—

"(A) whether the data is obtained as the information is being produced or from digital storage; and

"(B) where the vehicle data is stored or transmitted, including by wire or radio.

"(2) Consent.—The term 'consent'—

"(A) means an affirmative, express, and voluntary agreement that—

"(i) states that the person providing the consent is providing consent to a government official to access the digital contents, access credential, or online account information, or other information being sought;

"(ii) specifies the type of content, access credential, or online account information the person is providing access to;

"(iii) specifies the time period of the covered vehicle data to be accessed;

"(iv) informs the person providing consent that consent is optional and that the government official attempting to obtain consent must otherwise acquire a warrant if consent is not obtained;

"(v) does not involve sanctions or the threat of sanctions for withholding consent; and

"(vi) uses clear, simple, and comprehensible language that is presented in a way that is accessible to the person providing consent; and

"(B) does not include consent obtained through agreement to a generic privacy policy or a terms of service agreement.

"(3) Covered vehicle data.—The term 'covered vehicle data'—

"(A) means all onboard and telematics data generated by, processed by, or stored on a noncommercial vehicle using computing, storage, and communication systems installed, attached to, or carried in the vehicle, including diagnostic data, entertainment system data, navigation data, images or data captured by onboard sensors or cameras, including images or data used to support automated features or autonomous driving, internet access, and communication to and from vehicle occupants;

"(B) includes data gathered by event data recorders; and

"(C) does not include—

"(i) automotive software installed by the manufacturer, as defined by applicable industry standards or regulations;

"(ii) any data subject to [chapter 119](#) of this title or section 104 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1804](#)); or

"(iii) data that is collected from outside the vehicle, including speed data and geolocation data, for purposes of traffic, law enforcement, or toll collection.

"(4) Event data recorder.—The term 'event data recorder' has the meaning given that term in [section 563.5 of title 49](#), Code of Federal Regulations (as in effect on March 5, 2019).

"(5) Federal investigative or law enforcement officer.—The term 'Federal investigative or law enforcement officer' means any officer of the United States who is empowered by law to execute searches, to seize evidence, or to make arrests for a violation of any Federal law.

"(6) Noncommercial vehicle.—The term 'noncommercial vehicle' has the meaning given the term 'non-CMV' in [section 383.5 of title 49](#), Code of Federal Regulations.

"(7) Vehicle operator.—The term 'vehicle operator' means—

"(A) a person who controls the operation of a vehicle at the time consent is sought; and

"(B) with respect to a vehicle that is not classified as a highly autonomous vehicle by the Secretary of Transportation, the driver of the vehicle.

"Sec. 2731. Prohibition on Federal access to vehicle data.

"(a) In general.—Except as provided in subsection (b), a Federal investigative or law enforcement officer may not access covered vehicle data unless pursuant to a warrant issued in accordance with the procedures described in rule 41 of the Federal Rules of Criminal Procedure by a court of competent jurisdiction, or as otherwise provided in this chapter or sections 104 and 303 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1804](#), [1823](#)).

"(b) Exceptions.—

"(1) Consent.—

"(A) In general.—A Federal investigative or law enforcement officer may access covered vehicle data if—

"(i) the vehicle operator provides prior consent to such access; and

"(ii) no passenger 14 years of age or older objects to the access.

"(B) Vehicle owner.—If the vehicle operator cannot be located with reasonable effort, the vehicle owner or, in the case of a leased vehicle, the lessee, may provide consent under this paragraph.

"(C) Unlawful possession.—No individual may provide or withhold consent under this paragraph or object to another individual accessing covered vehicle data if the individual—

"(i) is the vehicle operator who is in unlawful possession of the vehicle; or

"(ii) is a passenger who unlawfully obtained access to the vehicle.

"(D) Oral consent.—Consent provided under this paragraph shall be in writing unless—

"(i) the person providing the consent requests that the consent be made orally; and

"(ii) the request for consent and the consent are recorded.

"(E) Consent of vehicle operator.—If the vehicle operator is not the owner of the vehicle and provides consent under this paragraph, the consent is valid only with respect to covered vehicle data generated during the lawful possession and use of the vehicle by the vehicle operator.

"(2) Emergency.—

"(A) In general.—A Federal investigative or law enforcement officer, the Attorney General, the Deputy Attorney General, or the Associate Attorney General may access covered vehicle data if—

"(i) such officer reasonably determines that an emergency situation exists that—

"(I) involves immediate danger of death or serious physical injury to any person; and

"(II) requires access to covered vehicle data before such officer can, with due diligence, obtain a warrant;

"(ii) there are grounds upon which a warrant could be granted to authorize such access; and

"(iii) an application for a warrant approving such access is submitted to a court within 48 hours after the access has occurred or begins to occur.

"(B) Denial.—If an application for a warrant submitted pursuant to subparagraph (A)(iii) is denied, any covered vehicle data accessed under this paragraph shall be treated as having been obtained in violation of this chapter.

"(3) Event data recorder for motor vehicle safety.—In addition to the exceptions in paragraphs (1) and (2), data recorded or transmitted by an event data recorder may be accessed from a noncommercial vehicle if authorized by paragraph (3), (4), or (5) of section 24302(b) of the Driver Privacy Act of 2015 ([49 U.S.C. 30101 note](#)).

"(4) Rule of construction.—Nothing in this section shall be interpreted to require the transmission or storage of data that is not otherwise transmitted or stored, or the retrieval of data that is not generally retrievable.

"Sec. 2732. Prohibition on use of acquired information as evidence.

"(a) In general.—If any covered vehicle data has been acquired in violation of this chapter, no part of such information and no evidence derived therefrom may be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding by, in, or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof.

"(b) Probable cause.—No data described in section 2731(b)(3) may be used to establish probable cause."

(2) Technical and conforming amendments.—

(A) Driver Privacy Act of 2015.—Section 24302 of the Driver Privacy Act of 2015 ([49 U.S.C. 30101 note](#)) is amended—

(i) in subsection (b), in the matter preceding paragraph (1), by striking "Data" and inserting "Except as provided in subsection (c), data"; and

(ii) by adding at the end the following:

"(c) Federal investigative or law enforcement officers.—A Federal investigative or law enforcement officer (as defined in section 2730 of title 18, United States Code) may only access or retrieve data recorded or transmitted by an event data recorder described in subsection (a) in accordance with chapter 124 of title 18, United States Code."

SEC. 105. THE FOURTH AMENDMENT IS NOT FOR SALE.

(a) Records held by data brokers.—[Section 2702 of title 18](#), United States Code, is amended by adding at the end the following:

"(e) Prohibition on obtaining in exchange for anything of value certain records and information by law enforcement and intelligence agencies.—

"(1) Definitions.—In this subsection:

"(A) the term 'biometric information'—

"(i) means any covered personal data that allows or confirms the unique identification or verification of an individual and is generated from the measurement or processing of unique biological, physical, or physiological characteristics, including—

"(I) fingerprints;

"(II) voice prints;

"(III) iris or retina imagery scans;

"(IV) facial or hand mapping, geometry, or templates; and

"(V) gait; and

"(ii) does not include—

"(I) a digital or physical photograph;

"(II) an audio or video recording; or

"(III) data derived from a digital or physical photograph or an audio or video recording that cannot be used to identify or authenticate a specific individual;

"(B) the term 'covered customer or subscriber record' means a covered record that is—

"(i) disclosed to any person or entity by—

"(I) an online service provider of which the covered person is a subscriber or customer; or

"(II) an intermediary or ancillary service provider that directly or indirectly delivers, transmits, stores, or processes communications or other covered personal data of such covered person;

"(ii) collected by any person or entity from an online account of a covered person; or

"(iii) collected by any person or entity from or about an electronic device of a covered person;

"(C) the term 'covered organization' means a person who—

"(i) is not a governmental entity; and

"(ii) is not an individual, unless such individual is an agent of, or otherwise acting on behalf of, a person who is not a governmental entity and is not an individual;

"(D) the term 'covered person' means—

"(i) a person who is located inside the United States; or

"(ii) a person—

"(I) who is located outside the United States or whose location cannot be determined; and

"(II) who is a United States person, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801](#));

"(E) the term 'covered personal data' means personal data relating to a covered person;

"(F) the term 'covered record'—

"(i) means a record or other information that—

"(I) relates to a covered person; and

"(II) is—

"(aa) a record or other information described in the matter preceding paragraph (1) of section 2703(c);

"(bb) the contents of a communication; or

"(cc) location information; and

"(ii) does not include a record or other information that—

"(I) has been voluntarily made available to the general public by a covered person on a social media platform or similar service;

"(II) is lawfully available to the public as a Federal, State, or local government record or through other widely distributed media;

"(III) is obtained by a law enforcement agency of a governmental entity or an element of the intelligence community for the purpose of conducting a background check of a covered person—

"(aa) with the written consent of such person;

"(bb) for access or use by such agency or element for the purpose of such background check; and

"(cc) that is destroyed after the date on which it is no longer needed for such background check; or

"(IV) is data generated by a public or private automated license plate recognition system;

"(G) the term 'electronic device' has the meaning given the term 'computer' in section 1030(e);

"(H) the term 'illegitimately obtained information' means a covered record that—

"(i) was obtained—

"(I) from an online service provider in a manner that—

"(aa) violates the service agreement between the provider and customers or subscribers of the provider; or

"(bb) is inconsistent with the privacy policy of the provider;

"(II) by deceiving the covered person whose covered record was obtained; or

"(III) through the unauthorized accessing of an electronic device or online account; or

"(ii) was—

"(I) obtained from an online service provider or an intermediary or ancillary service provider; and

"(II) collected, processed, or shared in violation of a contract relating to the covered record;

"(I) the term 'intelligence community' has the meaning given that term in section 3 of the National Security Act of 1947 ([50 U.S.C. 3003](#));

"(J) the term 'lawfully obtained public data' means covered personal data obtained by a particular covered organization—

"(i) that the covered organization reasonably understood to have been voluntarily made available to the general public by the covered person;

"(ii) that the covered organization obtained in compliance with all applicable laws and regulations; and

"(iii) if the covered organization did not initially obtain the covered personal data after the covered personal data was made available to the general public—

"(I) that the covered organization reasonably understood to have been obtained in compliance with all applicable laws and regulations by—

"(aa) the person that initially obtained the covered personal data; and

"(bb) if the covered organization did not obtain the covered personal data from the person described in item (aa), each other person in the sequence of transfers of the covered personal data leading up to the obtaining of the covered personal data by the covered organization; and

"(II) with respect to which the covered organization receives an attestation under penalty of perjury—

"(aa) by the person that initially obtained the covered personal data indicating that the covered personal data was voluntarily made available to the general public by the covered person and was obtained in compliance with all applicable laws and regulations; and

"(bb) if the covered organization did not obtain the covered personal data from the person described in item (aa), by each other person in the sequence of

transfers of the covered personal data leading up to the obtaining of the covered personal data by the covered organization indicating that such person reasonably understood the data to have been lawfully obtained public data;

"(K) the term 'location information' means information derived or otherwise calculated from the transmission or reception of a radio signal that reveals the approximate or actual geographic location of a customer, subscriber, user, or device;

"(L) the term 'obtain in exchange for anything of value' means to obtain by purchasing, to receive in connection with services being provided for monetary or nonmonetary consideration, or to otherwise obtain in exchange for consideration, including an access fee, service fee, maintenance fee, or licensing fee;

"(M) the term 'online account' means an online account with an online service provider; and

"(N) the term 'personal data'—

"(i) means data, derived data, or any unique identifier that is linked to, or is reasonably linkable to, an individual or to an electronic device that is linked to, or is reasonably linkable to 1 or more individuals in a household;

"(ii) includes anonymized data that, if combined with other data, can be linked to, or is reasonably linkable to, an individual or to an electronic device that identifies, is linked to, or is reasonably linkable to 1 or more individuals in a household; and

"(iii) does not include data that is lawfully available through Federal, State, or local government records or through widely distributed media.

"(2) Limitation.—

"(A) In general.—

"(i) Prohibition on covered personal data.—Subject to clauses (ii) through (vii), a law enforcement agency of a governmental entity or an element of the intelligence community may not obtain in exchange for anything of value covered personal data if—

"(I) the covered personal data is directly or indirectly obtained from a covered organization; or

"(II) the covered personal data is derived from covered personal data that was directly or indirectly obtained from a covered organization.

"(ii) Exception for certain compilations of data.—A law enforcement agency of a governmental entity or an element of the intelligence community may obtain in exchange for anything of value covered personal data as part of a larger compilation of data which includes personal data about persons who are not covered persons, if—

"(I) the law enforcement agency of a governmental entity or element of the intelligence community is unable through reasonable means to exclude covered personal data from the larger compilation obtained; and

"(II) the law enforcement agency of a governmental entity or element of the intelligence community minimizes any covered personal data from the larger compilation in accordance with the requirements described in paragraph (5).

"(iii) Exception for whistleblower disclosures to law enforcement.—Clause (i) shall not apply to covered personal data that is obtained by a law enforcement agency of a governmental entity or an element of the intelligence community under a program established by an Act of Congress under which a portion of a penalty or a similar payment or bounty is paid to an individual who discloses information about an unlawful activity to the Government, such as the program authorized under [section 7623](#) of the Internal Revenue Code of 1986.

"(iv) Exception for cost reimbursement under compulsory legal process.—Clause (i) shall not apply to covered personal data that is obtained by a law enforcement agency of a governmental entity or an element of the intelligence community from a covered organization in accordance with compulsory legal process that—

"(I) is established by statute; and

"(II) provides for the reimbursement of costs of the covered organization that are incurred in connection with providing the record or information to the law enforcement agency of a governmental entity or element of the intelligence community, such as the reimbursement of costs under [section 2706](#).

"(v) Exception for employment-related use.—Clause (i) shall not apply to covered personal data about an employee of, or applicant for employment by, a law enforcement agency of a governmental entity or an element of the intelligence community that is—

"(I) obtained by the law enforcement agency of a governmental entity or element of the intelligence community for lawful employment-related purposes;

"(II) accessed and used by the law enforcement agency of a governmental entity or element of the intelligence community only for such employment-related purposes; and

"(III) destroyed at such time as the covered personal data is no longer needed for employment-related purposes.

"(vi) Exception for use in background checks.—Clause (i) shall not apply to covered personal data about a covered person that is—

"(I) obtained by a law enforcement agency of a governmental entity or an element of the intelligence community for purposes of conducting a background check of the covered person with the written consent of the covered person;

"(II) accessed and used by the law enforcement agency of a governmental entity or element of the intelligence community only for background check-related purposes; and

"(III) destroyed at such time as the covered personal data is no longer needed for background check-related purposes.

"(vii) Exception for lawfully obtained public data.—

"(I) In general.—Except as provided in subclause (II) or (III), clause (i) shall not apply to covered personal data that is obtained by a law enforcement agency of a governmental entity or an element of the intelligence community if—

"(aa) the law enforcement agency of a governmental entity or element of the intelligence community reasonably believes that—

"(AA) the covered personal data is lawfully obtained public data; or

"(BB) the covered personal data is derived from covered personal data that solely consists of lawfully obtained public data; and

"(bb) the law enforcement agency of a governmental entity or element of the intelligence community receives—

"(AA) an attestation under penalty of perjury from the person providing the covered personal data that the covered personal data is lawfully obtained public data or is derived from covered personal data that solely consists of lawfully obtained public data; and

"(BB) each attestation described in paragraph (1)(J)(iii)(II) with respect to the lawfully obtained public data.

"(II) Exception for biometric information.—The exception under subclause (I) shall not apply to biometric information.

"(III) Exception for location information.—The exception under subclause (I) shall not apply to location information.

"(viii) Additional prohibition on covered customer or subscriber records and illegitimately obtained information.—A law enforcement agency of a governmental entity or an element of the intelligence community may not obtain in exchange for anything of value from any person or entity a covered customer or subscriber record or any illegitimately obtained information.

"(B) Indirectly acquired records and information.—The limitations under subparagraph (A) shall apply without regard to whether the covered organization or other person or entity possessing the covered personal data, covered customer or subscriber record, or illegitimately obtained information is the person or entity that initially obtained, collected, or received the disclosure of such data, record, or information.

"(3) Limit on sharing between agencies.—

"(A) In general.—A law enforcement agency of a governmental entity or an element of the intelligence community may not acquire, receive, query, or otherwise obtain or access covered personal data, a covered customer or subscriber record, or illegitimately obtained information from any governmental entity, if the covered personal data, covered customer or subscriber record, or illegitimately obtained information was obtained by that governmental entity in a manner that would violate paragraph (2) if the law enforcement

agency of a governmental entity or element of the intelligence community directly obtained the covered personal data, covered customer or subscriber record, or illegitimately obtained information in a like manner.

"(B) Causation not required.—The prohibition in subparagraph (A) shall apply without regard to whether the law enforcement agency of a governmental entity or element of the intelligence community caused the governmental entity to obtain the covered personal data, covered customer or subscriber record, or illegitimately obtained information.

"(C) Attestation required.—A law enforcement agency of a governmental entity or an element of the intelligence community may only acquire, receive, query, or otherwise obtain or access covered personal data, a covered customer or subscriber record, or illegitimately obtained information from another governmental entity if the law enforcement agency of a governmental entity or element of the intelligence community obtains an attestation that such data, record, or information was not obtained by that governmental entity in a manner that would violate paragraph (2) if the law enforcement agency of a governmental entity or element of the intelligence community directly obtained the data, record, or information in a like manner.

"(D) Destruction upon acquisition of knowledge.—If a law enforcement agency of a governmental entity or an element of the intelligence community learns that it previously acquired, queried, or otherwise obtained or accessed covered personal data, a covered customer or subscriber record, or illegitimately obtained information from any governmental entity that obtained such data, record, or information in a manner described in subparagraph (A), the law enforcement agency of a governmental entity or element of the intelligence community may not use or disseminate the data, record, or information or any information derived therefrom, and shall promptly destroy any such data, record, or information that is still retained.

"(4) Prohibition on use as evidence.—

"(A) In general.—Covered personal data, a covered customer or subscriber record, or illegitimately obtained information acquired, received, queried, or otherwise obtained or accessed by a law enforcement agency of a governmental entity or an element of the intelligence community in violation of paragraph (2) or (3), and any evidence derived therefrom, may not be used, received in evidence, or otherwise disseminated in any investigation, trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof.

"(B) Use by aggrieved parties.—Nothing in subparagraph (A) shall be construed to limit the use of covered personal data, a covered customer or subscriber record, or illegitimately obtained information by a covered person aggrieved by a violation of paragraph (2) or (3) in connection with any action relating to such a violation.

"(5) Minimization procedures.—

"(A) In general.—The Attorney General shall adopt specific procedures that are reasonably designed to minimize the acquisition and retention, and prohibit the

dissemination, of covered personal data, covered customer or subscriber records, and illegitimately obtained information acquired in violation of paragraph (2) or (3).

"(B) Use by agencies.—If a law enforcement agency of a governmental entity or an element of the intelligence community acquires covered personal data, a covered customer or subscriber record, or illegitimately obtained information in violation of paragraph (2) or (3), the agency or element shall minimize the acquisition and retention, and prohibit the dissemination, of such data, records, and information in accordance with the procedures adopted under subparagraph (A).".

(b) Required disclosure.—[Section 2703 of title 18](#), United States Code, as amended by this Act, is further amended by adding at the end the following:

"(n) Covered personal data.—

"(1) Definitions.—In this subsection, the terms 'covered organization' and 'covered personal data' have the meanings given such terms in [section 2702\(e\)](#).

"(2) Limitation.—Unless a governmental entity obtains an order in accordance with paragraph (3), the governmental entity may not require a covered organization that is not an online service provider to disclose covered personal data if a court order would be required for the governmental entity to require an online service provider to disclose such covered personal data that is a record of a customer or subscriber of the online service provider.

"(3) Orders.—

"(A) In general.—A court may only issue an order requiring a covered organization that is not an online service provider to disclose covered personal data on the same basis and subject to the same limitations as would apply to a court order to require disclosure by an online service provider.

"(B) Standard.—For purposes of subparagraph (A), a court shall apply the most stringent standard under Federal statute or the Constitution of the United States that would be applicable to a request for a court order to require a comparable disclosure by an online service provider of comparable records of a customer or subscriber of the online service provider.".

(c) Intermediary and ancillary service providers.—

(1) Definition.—Subsection (a) of [section 2711 of title 18](#), United States Code, as amended by this Act, is further amended by adding at the end the following:

"(9) the term 'intermediary or ancillary service provider' means an entity or facilities owner or operator that directly or indirectly delivers, transmits, stores, or processes communications or any other covered personal data (as defined in [section 2702\(e\)](#)) for, or on behalf of, an online service provider.".

(2) Prohibition.—[Section 2702\(a\) of title 18](#), United States Code, is amended—

(A) in paragraph (1), by striking "and" at the end;

(B) in paragraph (2)(B), by striking "and" at the end;

(C) in paragraph (3), by striking the period at the end and inserting "; and"; and

(D) by adding at the end the following:

"(4) an intermediary or ancillary service provider may not knowingly disclose—

"(A) to any person or entity the contents of a communication while in electronic storage by that intermediary or ancillary service provider; or

"(B) to any governmental entity a record or other information pertaining to a subscriber to or customer of, a recipient of a communication from a subscriber to or customer of, or the sender of a communication to a subscriber to or customer of, the online service provider for, or on behalf of, which the intermediary or ancillary service provider directly or indirectly delivers, transmits, stores, or processes communications or any other covered personal data (as defined in subsection (e)).".

(d) Limit on civil immunity for providing information, facilities, or technical assistance to the Government absent a court order.—[Section 2511\(2\)\(a\) of title 18](#), United States Code, is amended—

(1) in subparagraph (ii), by striking clause (B) and inserting the following:

"(B) a certification in writing—

"(I) by a person specified in [section 2518\(7\)](#) or the Attorney General of the United States;

"(II) that the requirements for an emergency authorization to intercept a wire, oral, or electronic communication under [section 2518\(7\)](#) have been met; and

"(III) that the specified assistance is required,"; and

(2) by striking subparagraph (iii) and inserting the following:

"(iii) For assistance provided pursuant to a certification under subparagraph (ii)(B), the limitation on causes of action under the last sentence of the matter following subparagraph (ii)(B) shall only apply to the extent that the assistance ceased at the earliest of the time the application for a court order was denied, the time the communication sought was obtained, or 48 hours after the interception began.".

SEC. 106. ELIGIBILITY FOR BYRNE GRANT PROGRAM.

(a) Requirements for Byrne grant eligibility.—Beginning in the 2028 fiscal year, except as permitted by subsection (b), a State or unit of local government (other than an Indian Tribe) may not receive funds under the Byrne grant program for that fiscal year unless, on the day before the first day of the fiscal year, the State or unit of local government—

(1) has submitted the required records to the National Police Misconduct Registry established under section 189;

(2) has submitted to the Attorney General evidence that the State or unit of local government has a certification and decertification program for purposes of employment as a

law enforcement officer in that State or unit of local government which is consistent with the rules made under section 188;

(3) (A) has submitted to the Attorney General the percentage of people released after a sentence of more than 1 year who had valid photo identification during the 12 months ending June 30 of that year; and

(B) achieved a percentage above the threshold for the upcoming fiscal year:

(i) for fiscal year 2028, 25 percent;

(ii) for fiscal year 2029, 80 percent;

(iii) for fiscal year 2030 and beyond, 97 percent; and

(4) (A) has submitted to the Attorney General the percentage of criminal cases where payment of money was a condition of pretrial release during the 12 months ending June 30 of that year; and

(B) achieved a percentage below the threshold for the upcoming fiscal year:

(i) for fiscal year 2028, 75 percent;

(ii) for fiscal year 2029, 50 percent;

(iii) for fiscal year 2030, 25 percent;

(iv) for fiscal year 2031 and beyond, 10 percent.

(5) has implemented, for all courts of record of the State or unit of local government, a system under which—

(A) each precedential judicial opinion and order is assigned a neutral citation (as such term is defined in section 153 of the POPULIST Act); and

(B) such neutral citation is sufficient by itself for citation in all courts of the State or unit of local government and is not required to be accompanied by a proprietary reporter citation.

(b) Partial eligibility.—A State or unit of local government who is ineligible for the Byrne grant program solely as a result of not fully meeting the eligibility criteria in subsection (a) may receive a partial grant. Notwithstanding the provisions of [section 10156 of title 34](#), United States Code, any grant authorized by this subsection shall not exceed a percentage of the amount of the Byrne grant in the previous fiscal year, calculated as the sum of the following—

(1) for compliance with (a)(1), 20 percent;

(2) for compliance with (a)(2), 25 percent;

(3) for compliance with (a)(3), 20 percent;

(4) for compliance with (a)(4), 20 percent;

(5) for compliance with (a)(5)(A), 10 percent; and

(6) for compliance with (a)(5)(B), 15 percent.

Subtitle A—Jubilee Reform

SEC. 111. FINDINGS AND PURPOSE.

(a) Findings.—Congress finds the following:

(1) The concept of a jubilee, drawn from the biblical tradition, recognized that societies accumulate not only financial obligations but also moral debts that must regularly be forgiven. Such jubilees, said to occur every 50 years, proclaimed liberty throughout the land, included the release of those held in enslavement or incarceration.

(2) As the United States marks its 250th birthday, a national jubilee is an opportunity to confront moral failures such as our system of mass incarceration, which has inflicted lasting harm on individuals, families, and communities and stands as a spiritual stain on the soul of the United States of America.

(3) Federal sentencing policy adopted over the last 4 decades, including mandatory minimum penalties and rigid sentencing frameworks, has produced excessive and disproportionate terms of imprisonment, shifted power away from judges toward inflexible statutory rules, and undermined the Constitutional goal of individualized justice.

(4) Extended incarceration yields sharply diminishing public safety returns after substantial time served, while imposing escalating human, fiscal, and institutional costs, including the maintenance of a large aging prison population that poses little risk to public safety and requires increasingly expensive medical and custodial care.

(5) The abolition of Federal parole eliminated individualized and ongoing review of incarceration decisions, replacing it with fixed sentencing assumptions made at a single point in time, regardless of later maturation, rehabilitation, changed circumstances, or demonstrated readiness for reintegration.

(6) Parole and second-look mechanisms conditioned on conduct, rehabilitation, and public safety promote accountability rather than leniency, reinforce respect for the law, and better align punishment with the Constitutional purposes of sentencing than irreversible and inflexible incarceration schemes. Retroactive application is necessary to restore equal treatment under law.

(7) The continued operation of the Guantanamo Bay military prison, including the prolonged detention of individuals without charge or trial, represents a continuing failure of justice, departs from Constitutional principles, due process, and the rule of law, and has caused lasting damage to the moral authority of the United States at home and abroad.

(8) Congress has the authority and the responsibility to correct systemic injustices it has created, including unjust sentencing regimes and unlawful detention practices, and to restore liberty in a manner consistent with public safety, Constitutional values, and human dignity.

(b) Purpose.—The purposes of this subtitle are—