

(b) American Value Fund.—99 percent of all amounts deposited pursuant to subsection (a) shall be credited to the American Value Fund established in title VI of the POPULIST Act.

(c) United States Patent and Trademark Office.—1 percent of all amounts deposited pursuant to subsection (a) shall be transferred to the United States Patent and Trademark Office and shall be available, without further appropriation, solely for trademark examination, registry maintenance, fraud detection, enforcement of use requirements, and administrative modernization.

(d) Budgetary treatment.—Amounts transferred under this section shall be treated as offsetting receipts for purposes of the Congressional Budget Act of 1974 ([2 U.S.C. 621 et seq.](#)).

Subtitle D—Data Privacy and Protection

SEC. 561. DEFINITIONS.

(a) Definitions.—In this subtitle:

(1) Affirmative express consent.—

(A) In general.—The term "affirmative express consent" means an affirmative act by an individual that clearly communicates the individual's freely given, specific, and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a covered entity that meets the requirements of subparagraph (B).

(B) Request requirements.—The requirements of this subparagraph with respect to a request from a covered entity to an individual are the following:

(i) The request is provided to the individual in a clear and conspicuous standalone disclosure made through the primary medium used to offer the covered entity's product or service, or only if the product or service is not offered in a medium that permits the making of the request under this paragraph, another medium regularly used in conjunction with the covered entity's product or service.

(ii) The request includes a description of the processing purpose for which the individual's consent is sought and—

(I) clearly states the specific categories of covered data that the covered entity shall collect, process, and transfer necessary to effectuate the processing purpose; and

(II) includes a prominent heading and is written in easy-to-understand language that would enable a reasonable individual to identify and understand the processing purpose for which consent is sought and the covered data to be collected, processed, or transferred by the covered entity for such processing purpose.

(iii) The request clearly explains the individual's applicable rights related to consent.

(iv) The request is made in a manner reasonably accessible to and usable by individuals with disabilities.

(v) The request is made available to the individual in each covered language in which the covered entity provides a product or service for which authorization is sought.

(vi) The option to refuse consent shall be at least as prominent as the option to accept, and the option to refuse consent shall take the same number of steps or fewer as the option to accept.

(vii) Processing or transferring any covered data collected pursuant to affirmative express consent for a different processing purpose than that for which affirmative express consent was obtained shall require affirmative express consent for the subsequent processing purpose.

(C) Express consent required.—A covered entity may not infer that an individual has provided affirmative express consent to an act or practice from—

(i) the inaction of the individual;

(ii) the individual's continued use of a service or product provided by the covered entity; or

(iii) the individual's approval of a preselected default option.

(D) Pretextual consent prohibited.—A covered entity may not obtain or attempt to obtain the affirmative express consent of an individual through—

(i) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(ii) the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to provide such consent or any covered data.

(2) Authentication.—The term "authentication" means the process of verifying an individual or entity for security purposes.

(3) Biometric information.—

(A) In general.—The term "biometric information" means any covered data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual, including—

(i) fingerprints;

(ii) voice prints;

(iii) iris or retina scans;

(iv) facial or hand mapping, geometry, or templates; or

(v) gait or personally identifying physical movements.

(B) Exclusion.—The term "biometric information" does not include—

- (i) a digital or physical photograph;
- (ii) an audio or video recording; or
- (iii) data generated from a digital or physical photograph, or an audio or video recording, that cannot be used to identify an individual.

(4) Child.—The term "child" means a covered minor under 13 years of age.

(5) Collect; collection.—The terms "collect" and "collection" mean buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means.

(6) Commission.—The term "Commission" means the Federal Trade Commission.

(7) Control.—The term "control" means, with respect to an entity—

(A) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of the entity;

(B) control over the election of a majority of the directors of the entity (or of individuals exercising similar functions); or

(C) the power to exercise a controlling influence over the management of the entity.

(8) Covered algorithm.—The term "covered algorithm" means a computational process that uses machine learning, natural language processing, artificial intelligence techniques, or other computational processing techniques of similar or greater complexity and that makes a decision or facilitates human decision making with respect to covered data, including to determine the provision of products or services or to rank, order, promote, recommend, amplify, or similarly determine the delivery or display of information to an individual.

(9) Covered data.—

(A) In general.—The term "covered data" means information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual, and may include derived data and unique persistent identifiers.

(B) Exclusions.—The term "covered data" does not include—

(i) de-identified data;

(ii) employee data;

(iii) publicly available information; or

(iv) inferences made exclusively from multiple independent sources of publicly available information that do not reveal sensitive covered data with respect to an individual.

(C) Employee data defined.—For purposes of subparagraph (B), the term "employee data" means—

(i) information relating to a job applicant collected by a covered entity acting as a prospective employer of such job applicant in the course of the application, or hiring process, if such information is collected, processed, or transferred by the prospective employer solely for purposes related to the employee's status as a current or former job applicant of such employer;

(ii) information processed by an employer relating to an employee who is acting in a professional capacity for the employer, provided that such information is collected, processed, or transferred solely for purposes related to such employee's professional activities on behalf of the employer;

(iii) the business contact information of an employee, including the employee's name, position or title, business telephone number, business address, or business email address that is provided to an employer by an employee who is acting in a professional capacity, if such information is collected, processed, or transferred solely for purposes related to such employee's professional activities on behalf of the employer;

(iv) emergency contact information collected by an employer that relates to an employee of that employer, if such information is collected, processed, or transferred solely for the purpose of having an emergency contact on file for the employee and for processing or transferring such information in case of an emergency; or

(v) information relating to an employee (or a spouse, dependent, other covered family member, or beneficiary of such employee) that is necessary for the employer to collect, process, or transfer solely for the purpose of administering benefits to which such employee (or spouse, dependent, other covered family member, or beneficiary of such employee) is entitled on the basis of the employee's position with that employer.

(10) Covered entity.—

(A) In general.—The term "covered entity"—

(i) means any entity or any person, other than an individual acting in a noncommercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data and—

(I) is subject to the Federal Trade Commission Act ([15 U.S.C. 41 et seq.](#));

(II) is a common carrier subject to the Communications Act of 1934 ([47 U.S.C. 151 et seq.](#)) and all Acts amendatory thereof and supplementary thereto; or

(III) is an organization not organized to carry on business for its own profit or that of its members; and

(ii) includes any entity or person that controls, is controlled by, or is under common control with the covered entity.

(B) Exclusions.—The term "covered entity" does not include—

(i) a Federal, State, Tribal, territorial, or local government entity such as a body, authority, board, bureau, commission, district, agency, or political subdivision of the Federal Government or a State, Tribal, territorial, or local government;

(ii) a person or an entity that is collecting, processing, or transferring covered data on behalf of a Federal, State, Tribal, territorial, or local government entity, in so far as such person or entity is acting as a service provider to such government entity, provided that such person or entity shall remain subject to all requirements of this subtitle applicable to service providers; or

(iii) an entity that serves as a congressionally designated nonprofit, national resource center, and clearinghouse to provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children issues.

(C) Nonapplication to service providers.—An entity shall not be considered to be a covered entity for purposes of this subtitle in so far as the entity is acting as a service provider.

(11) Covered language.—The term "covered language" means the 10 languages with the most users in the United States, according to the most recent United States Census.

(12) Covered minor.—The term "covered minor" means an individual under the age of 17.

(13) De-identified data.—The term "de-identified data" means information that does not identify and is not linked or reasonably linkable to a distinct individual or a device, regardless of whether the information is aggregated, and if the covered entity or service provider—

(A) takes reasonable technical measures to ensure that the information cannot, at any point, be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual;

(B) publicly commits in a clear and conspicuous manner—

(i) to process and transfer the information solely in a de-identified form without any reasonable means for re-identification; and

(ii) to not attempt to re-identify the information with any individual or device that identifies or is linked or reasonably linkable to an individual; and

(C) contractually obligates any person or entity that receives the information from the covered entity or service provider—

(i) to comply with all of the provisions of this paragraph with respect to the information; and

(ii) to require that such contractual obligations be included contractually in all subsequent instances for which the data may be received.

(14) Derived data.—The term "derived data" means covered data that is created by the derivation of information, data, assumptions, correlations, inferences, predictions, or

conclusions from facts, evidence, or another source of information or data about an individual or an individual's device.

(15) Device.—The term "device" means any electronic equipment capable of collecting, processing, or transferring covered data that is used by 1 or more individuals.

(16) Employee.—The term "employee" means an individual who is an employee, director, officer, staff member, or individual working as an independent contractor that is not a service provider, trainee, volunteer, or intern of an employer, regardless of whether such individual is paid, unpaid, or employed on a temporary basis.

(17) Executive agency.—The term "Executive agency" has the meaning given such term in [section 105 of title 5](#), United States Code.

(18) First party advertising or marketing.—The term "first party advertising or marketing" means advertising or marketing conducted by a first party either through direct communications with a user such as direct mail, email, or text message communications, or advertising or marketing conducted entirely within the first-party context, such as in a physical location operated by the first party, or on a web site or app operated by the first party.

(19) Genetic information.—The term "genetic information" means any covered data, regardless of its format, that concerns an individual's genetic characteristics, including—

(A) raw sequence data that results from the sequencing of the complete, or a portion of the, extracted deoxyribonucleic acid (DNA) of an individual; or

(B) genotypic and phenotypic information that results from analyzing raw sequence data described in subparagraph (A).

(20) Individual.—The term "individual" means a natural person residing in the United States.

(21) Knowledge.—

(A) In general.—The term "knowledge", with respect to whether an individual is a covered minor, means actual knowledge or knowledge fairly implied on the basis of objective circumstances.

(B) Rule of construction.—Nothing in this subtitle, including subparagraph (A), shall be construed to require a covered entity or service provider to—

(i) affirmatively collect any covered data with respect to age that the covered entity or service provider is not otherwise collecting in the normal course of business; or

(ii) implement age-gating or age-verification functionality.

(C) Guidance.—Not later than January 1, 2027, the Commission shall issue guidance, including best practices and examples, to assist covered entities and service providers in determining whether they have knowledge fairly implied on the basis of objective circumstances that an individual is a covered minor.

(22) Large data holder.—

(A) In general.—The term "large data holder" means a covered entity or service provider that, in the most recent calendar year—

(i) had annual gross revenues of \$250,000,000 or more; and

(ii) collected, processed, or transferred—

(I) the covered data of more than 5,000,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals, excluding covered data collected and processed solely for the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested product or service; or

(II) the sensitive covered data of more than 200,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals.

(B) Exclusions.—The term "large data holder" does not include any instance in which the covered entity or service provider would qualify as a large data holder solely on the basis of collecting or processing—

(i) personal email addresses;

(ii) personal telephone numbers; or

(iii) log-in information of an individual or device to allow the individual or device to log in to an account administered by the covered entity or service provider.

(C) Revenue.—For purposes of determining whether any covered entity or service provider is a large data holder, the term "revenue", with respect to any covered entity or service provider that is not organized to carry on business for its own profit or that of its members—

(i) means the gross receipts the covered entity or service provider received, in whatever form, from all sources, without subtracting any costs or expenses; and

(ii) includes contributions, gifts, grants, dues or other assessments, income from investments, and proceeds from the sale of real or personal property.

(23) Market research.—The term "market research" means the collection, processing, or transfer of covered data as reasonably necessary and proportionate to investigate the market for or marketing of products, services, or ideas, where the covered data is not—

(A) integrated into any product or service;

(B) otherwise used to contact any individual or individual's device; or

(C) used to advertise or market to any individual or individual's device.

(24) Material.—The term "material" means, with respect to an act, practice, or representation of a covered entity (including a representation made by the covered entity in a privacy policy or similar disclosure to individuals) involving the collection, processing, or

transfer of covered data, that such act, practice, or representation is likely to affect a reasonable individual's decision or conduct regarding a product or service.

(25) Online product or service.—The term "online product or service" means a website, online service, online application, or mobile application.

(26) Parent.—The term "parent" means a parent or legal guardian.

(27) Person.—The term "person" has the meaning given the term in subsection (a) of section 1 of the Clayton Act ([15 U.S.C. 12](#)).

(28) Precise geolocation information.—

(A) In general.—The term "precise geolocation information" means information that is derived from a device or technology that reveals the past or present physical location of an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals, with sufficient precision to identify street level location information of an individual or device or the location of an individual or device within a range of 1,850 feet or less.

(B) Exclusion.—The term "precise geolocation information" does not include geolocation information identifiable or derived solely from the visual content of a legally obtained image, including the location of the device that captured such image.

(29) Process.—The term "process" means to conduct or direct any operation or set of operations performed on covered data, including analyzing, organizing, structuring, retaining, storing, using, or otherwise handling covered data.

(30) Processing purpose.—The term "processing purpose" means a reason for which a covered entity or service provider collects, processes, or transfers covered data that is specific and granular enough for a reasonable individual to understand the material facts of how and why the covered entity or service provider collects, processes, or transfers the covered data.

(31) Publicly available information.—

(A) In general.—The term "publicly available information" means any information that a covered entity or service provider has a reasonable basis to believe has been lawfully made available to the general public from—

(i) Federal, State, or local government records, if the covered entity collects, processes, and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity;

(ii) widely distributed media;

(iii) a website or online service made available to all members of the public, for free or for a fee, including where all members of the public, for free or for a fee, can log in to the website or online service;

(iv) a disclosure that has been made to the general public as required by Federal, State, or local law; or

(v) the visual observation of the physical presence of an individual or a device in a public place, not including data collected by a device in the individual's possession.

(B) Clarifications; limitations.—

(i) Available to all members of the public.—For purposes of this paragraph, information from a website or online service is not available to all members of the public if the individual who made the information available via the website or online service has restricted the information to a specific audience.

(ii) Other limitations.—The term "publicly available information" does not include—

(I) any obscene visual depiction (as defined in [section 1460 of title 18](#), United States Code);

(II) any inference made exclusively from multiple independent sources of publicly available information that reveals sensitive covered data with respect to an individual;

(III) biometric information;

(IV) publicly available information that has been combined with covered data;

(V) genetic information, unless otherwise made available by the individual to whom the information pertains as described in clause (ii) or (iii) of subparagraph (A); or

(VI) intimate images known to be nonconsensual.

(32) Sensitive covered data.—

(A) In general.—The term "sensitive covered data" means the following types of covered data:

(i) A government-issued identifier, such as a Social Security number, passport number, or driver's license number, that is not required by law to be displayed in public.

(ii) Any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or health care condition or treatment of an individual.

(iii) A financial account number, debit card number, credit card number, or information that describes or reveals the income level or bank account balances of an individual, except that the last 4 digits of a debit or credit card number shall not be deemed sensitive covered data.

(iv) Biometric information.

(v) Genetic information.

(vi) Precise geolocation information.

(vii) An individual's private communications such as voicemails, emails, texts, direct messages, or mail, or information identifying the parties to such communications, voice communications, video communications, and any information that pertains to the transmission of such communications, including telephone numbers called, telephone numbers from which calls were placed, the time calls were made, call duration, and location information of the parties to the call, unless the covered entity or a service provider acting on behalf of the covered entity is the sender or an intended recipient of the communication. Communications are not private for purposes of this clause if such communications are made from or to a device provided by an employer to an employee insofar as such employer provides conspicuous notice that such employer may access such communications.

(viii) Account or device log-in credentials, or security or access codes for an account or device.

(ix) Information identifying the sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding the collection, processing, or transfer of such information.

(x) Calendar information, address book information, phone or text logs, photos, audio recordings, or videos, maintained for private use by an individual, regardless of whether such information is stored on the individual's device or is accessible from that device and is backed up in a separate location. Such information is not sensitive for purposes of this paragraph if such information is sent from or to a device provided by an employer to an employee insofar as such employer provides conspicuous notice that it may access such information.

(xi) A photograph, film, video recording, or other similar medium that shows the naked or undergarment-clad private area of an individual.

(xii) Information revealing the video content requested or selected by an individual collected by a covered entity that is not a provider of a service described in section 562(b)(6). This clause does not include covered data used solely for transfers for independent video measurement.

(xiii) Information about an individual when the covered entity or service provider has knowledge that the individual is a covered minor.

(xiv) An individual's race, color, ethnicity, religion, or union membership.

(xv) Information identifying an individual's online activities over time and across third-party websites or online services.

(xvi) Any other covered data collected, processed, or transferred for the purpose of identifying the types of covered data listed in clauses (i) through (xv).

(B) Rulemaking.—The Commission may commence a rulemaking pursuant to [section 553 of title 5](#), United States Code, to include in the definition of "sensitive covered data" any other type of covered data that may require a similar level of protection as the types of

covered data listed in clauses (i) through (xvi) of subparagraph (A) as a result of any new method of collecting, processing, or transferring covered data.

(33) Service provider.—

(A) In general.—The term "service provider" means a person or entity that—

(i) collects, processes, or transfers covered data on behalf of, and at the direction of, a covered entity or a Federal, State, Tribal, territorial, or local government entity; and

(ii) receives covered data from or on behalf of a covered entity or a Federal, State, Tribal, territorial, or local government entity.

(B) Treatment with respect to service provider data.—A service provider that receives service provider data from another service provider as permitted under this subtitle shall be treated as a service provider under this subtitle with respect to such data.

(34) Service provider data.—The term "service provider data" means covered data that is collected or processed by or has been transferred to a service provider by or on behalf of a covered entity, a Federal, State, Tribal, territorial, or local government entity, or another service provider for the purpose of allowing the service provider to whom such covered data is transferred to perform a service or function on behalf of, and at the direction of, such covered entity or Federal, State, Tribal, territorial, or local government entity.

(35) State.—The term "State" means any of the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands of the United States, Guam, American Samoa, or the Commonwealth of the Northern Mariana Islands.

(36) State privacy authority.—The term "State privacy authority" means—

(A) the chief consumer protection officer of a State; or

(B) a State consumer protection agency with expertise in data protection, including the California Privacy Protection Agency.

(37) Substantial privacy risk.—The term "substantial privacy risk" means the collection, processing, or transfer of covered data in a manner that may result in any reasonably foreseeable substantial physical injury, economic injury, highly offensive intrusion into the privacy expectations of a reasonable individual under the circumstances, or discrimination on the basis of race, color, religion, national origin, sex, or disability.

(38) Targeted advertising.—The term "targeted advertising"—

(A) means presenting to an individual or device identified by a unique identifier, or groups of individuals or devices identified by unique identifiers, an online advertisement that is selected based on known or predicted preferences, characteristics, or interests associated with the individual or a device identified by a unique identifier; and

(B) does not include—

(i) advertising or marketing to an individual or an individual's device in response to the individual's specific request for information or feedback;

(ii) contextual advertising, which is when an advertisement is displayed based on the content in which the advertisement appears and does not vary based on who is viewing the advertisement; or

(iii) processing covered data solely for measuring or reporting advertising or content, performance, reach, or frequency, including independent measurement.

(39) Third party.—The term "third party"—

(A) means any person or entity, including a covered entity, that—

(i) collects, processes, or transfers covered data that the person or entity did not collect directly from the individual linked or linkable to such covered data; and

(ii) is not a service provider with respect to such data; and

(B) does not include a person or entity that collects covered data from another entity if the 2 entities are related by common ownership or corporate control, but only if a reasonable consumer's reasonable expectation would be that such entities share information.

(40) Third-party collecting entity.—

(A) In general.—The term "third-party collecting entity"—

(i) means a covered entity whose principal source of revenue is derived from processing or transferring covered data that the covered entity did not collect directly from the individuals linked or linkable to the covered data; and

(ii) does not include a covered entity insofar as such entity processes employee data collected by and received from a third party concerning any individual who is an employee of the third party for the sole purpose of such third party providing benefits to the employee.

(B) Principal source of revenue defined.—For purposes of this paragraph, the term "principal source of revenue" means, for the prior 12-month period, either—

(i) more than 50 percent of all revenue of the covered entity; or

(ii) obtaining revenue from processing or transferring the covered data of more than 5,000,000 individuals that the covered entity did not collect directly from the individuals linked or linkable to the covered data.

(C) Nonapplication to service providers.—An entity may not be considered to be a third-party collecting entity for purposes of this subtitle if the entity is acting as a service provider.

(41) Third-party data.—The term "third-party data" means covered data that has been transferred to a third party.

(42) Transfer.—The term "transfer" means to disclose, release, disseminate, make available, license, rent, or share covered data orally, in writing, electronically, or by any other means.

(43) Unique identifier.—The term "unique identifier"—

(A) means an identifier to the extent that such identifier is reasonably linkable to an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals, including a device identifier, Internet Protocol address, cookie, beacon, pixel tag, mobile ad identifier, or similar technology, customer number, unique pseudonym, user alias, telephone number, or other form of persistent or probabilistic identifier that is linked or reasonably linkable to an individual or device; and

(B) does not include an identifier assigned by a covered entity for the specific purpose of giving effect to an individual's exercise of affirmative express consent, or of opt-outs or other limits, with respect to the collection, processing, or transfer of such information.

(44) Widely distributed media.—The term "widely distributed media" means information that is available to the general public, including information from a telephone book or online directory, a television, internet, or radio program, the news media, or an internet site that is available to the general public on an unrestricted basis, but does not include an obscene visual depiction (as defined in [section 1460 of title 18](#), United States Code).

SEC. 562. DATA MINIMIZATION AND LOYALTY OBLIGATIONS.

(a) Data minimization.—

(1) In general.—A covered entity may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to—

(A) provide or maintain a specific product or service requested by the individual to whom the data pertains; or

(B) effect a purpose permitted under paragraph (2).

(2) Permissible purposes.—A covered entity may collect, process, or transfer covered data for any of the following purposes if the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to such purpose:

(A) To initiate, manage, or complete a transaction or fulfill an order for specific products or services requested by an individual, including any associated routine administrative, operational, and account servicing activity such as billing, shipping, delivery, storage, and accounting.

(B) With respect to covered data previously collected in accordance with this subtitle, notwithstanding this exception—

(i) to process such data as necessary to perform system maintenance or diagnostics;

(ii) to develop, maintain, repair, or enhance a product or service for which such data was collected;

(iii) to conduct internal research or analytics to improve a product or service for which such data was collected;

(iv) to perform inventory management or reasonable network management;

(v) to protect against spam; or

(vi) to debug or repair errors that impair the functionality of a service or product for which such data was collected.

(C) To authenticate users of a product or service.

(D) To fulfill a product or service warranty.

(E) To prevent, detect, protect against, or respond to a security incident. For purposes of this subparagraph, security is defined as network security and physical security and life safety, including an intrusion or trespass, medical alerts, fire alarms, and access control security.

(F) To prevent, detect, protect against, or respond to fraud, harassment, or illegal activity. For purposes of this subparagraph, the term "illegal activity" means a violation of a Federal, State, or local law punishable as a felony or misdemeanor that can directly harm another person.

(G) To comply with a legal obligation imposed by Federal, Tribal, local, or State law, or to investigate, establish, prepare for, exercise, or defend legal claims involving the covered entity or service provider.

(H) To prevent an individual, or group of individuals, from suffering harm where the covered entity or service provider believes in good faith that the individual, or group of individuals, is at risk of death, serious physical injury, or other serious health risk.

(I) To effectuate a product recall pursuant to Federal or State law.

(J) (i) To conduct a public or peer-reviewed scientific, historical, or statistical research project that—

(I) is in the public interest; and

(II) adheres to all relevant laws and regulations governing such research, including regulations for the protection of human subjects, or is excluded from criteria of the institutional review board.

(ii) Not later than July 1, 2027, the Commission shall issue guidelines to help covered entities ensure the privacy of affected users and the security of covered data, particularly as data is being transferred to and stored by researchers. Such guidelines should consider risks as they pertain to projects using covered data with special considerations for projects that are exempt under [part 46 of title 45](#), Code of Federal

Regulations (or any successor regulation) or are excluded from the criteria for institutional review board review.

(K) To deliver a communication that is not an advertisement to an individual, if the communication is reasonably anticipated by the individual within the context of the individual's interactions with the covered entity.

(L) To deliver a communication at the direction of an individual between such individual and 1 or more individuals or entities.

(M) To transfer assets to a third party in the context of a merger, acquisition, bankruptcy, or similar transaction when the third party assumes control, in whole or in part, of the covered entity's assets, only if the covered entity, in a reasonable time prior to such transfer, provides each affected individual with—

(i) a notice describing such transfer, including the name of the entity or entities receiving the individual's covered data and their privacy policies as described in section 563(b); and

(ii) a reasonable opportunity to withdraw any previously given consents in accordance with the requirements of affirmative express consent under this subtitle related to the individual's covered data and a reasonable opportunity to request the deletion of the individual's covered data, as described in section 563(c).

(N) To ensure the data security and integrity of covered data, as described in section 564(a).

(O) With respect to covered data previously collected in accordance with this subtitle, a service provider acting at the direction of a government entity, or a service provided to a government entity by a covered entity, and only insofar as authorized by statute, to prevent, detect, protect against or respond to a public safety incident, including trespass, natural disaster, or national security incident. This subparagraph does not permit, however, the transfer of covered data for payment or other valuable consideration to a government entity.

(P) With respect to covered data collected in accordance with this subtitle, notwithstanding this exception, to process such data as necessary to provide non-targeted first party advertising or marketing of products or services provided by the covered entity for individuals who are not covered minors.

(3) Guidance.—Not later than July 1, 2027, the Commission shall issue guidance regarding what is reasonably necessary and proportionate to comply with this subsection. Such guidance shall take into consideration—

(A) the size of, and the nature, scope, and complexity of the activities engaged in by, the covered entity, including whether the covered entity is a large data holder, nonprofit organization, covered entity meeting the requirements of section 563(e)(2), third party, or third-party collecting entity;

(B) the sensitivity of covered data collected, processed, or transferred by the covered entity;

(C) the volume of covered data collected, processed, or transferred by the covered entity; and

(D) the number of individuals and devices to which the covered data collected, processed, or transferred by the covered entity relates.

(4) Deceptive marketing.—A covered entity or service provider may not engage in deceptive advertising or marketing with respect to a product or service offered to an individual.

(5) Journalism.—Nothing in this subtitle shall be construed to limit or diminish First Amendment freedoms guaranteed under the Constitution.

(b) Loyalty duties.—Notwithstanding subsection (a) and unless an exception applies, with respect to covered data, a covered entity or service provider may not—

(1) collect, process, or transfer a Social Security number, except when necessary to facilitate an extension of credit, authentication, fraud and identity fraud detection and prevention, the payment or collection of taxes, the enforcement of a contract between parties, or the prevention, investigation, or prosecution of fraud or illegal activity, or as otherwise required by Federal, State, or local law;

(2) transfer covered data to a third party unless—

(A) the transfer is strictly necessary to provide a specific product or service requested by the individual to whom the covered data pertains;

(B) the transfer is made pursuant to the affirmative express consent of the individual;

(C) the transfer is strictly necessary to effect a purpose enumerated in subsection (a)(2)(E) through (O);

(D) with respect to a covered minor and subject to paragraph (5), the entity or service provider has knowledge that the individual is a covered minor and the transfer is made—

(i) pursuant to affirmative express consent obtained from—

(I) the covered minor, provided such minor is not a child; or

(II) the covered minor's parent; or

(ii) solely in order to submit information relating to victimization of a covered minor to law enforcement or an entity described in section 561(a)(10)(B)(iii); or

(E) the transfer is expressly required by Federal, State, Tribal, or local law;

(3) transfer covered data to a Federal, State, Tribal, territorial, or local government entity, or to any foreign governmental entity, unless—

(A) the transfer is made pursuant to a search warrant;

(B) the transfer is expressly required by Federal, State, Tribal, territorial, or local law;

(C) the transfer is strictly necessary to prevent or respond to an imminent threat of death or serious physical injury; or

(D) the transfer is strictly necessary to effect a purpose enumerated in subsection (a)(2)(E), (G), (H), (I), or (O);

provided that a transfer under this paragraph may not be made for payment or other valuable consideration, except for reimbursement of reasonable costs incurred;

(4) collect or process sensitive covered data, except where such collection or processing is strictly necessary to provide or maintain a specific product or service requested by the individual to whom the covered data pertains, or is strictly necessary to effect a purpose enumerated in subsection (a)(2)(A) through (L) and (N) through (O);

(5) transfer an individual's sensitive covered data to a third party, unless—

(A) the transfer is made pursuant to the affirmative express consent of the individual;

(B) the transfer is necessary to comply with a legal obligation imposed by Federal, State, Tribal, or local law, or to establish, exercise, or defend legal claims;

(C) the transfer is necessary to prevent an individual from imminent injury where the covered entity believes in good faith that the individual is at risk of death, serious physical injury, or serious health risk;

(D) with respect to covered data collected in accordance with this subtitle, notwithstanding this exception, a service provider acting at the direction of a government entity, or a service provided to a government entity by a covered entity, and only insofar as authorized by statute, the transfer is necessary to prevent, detect, protect against or respond to a public safety incident including trespass, natural disaster, or national security incident. This paragraph does not permit, however, the transfer of covered data for payment or other valuable consideration to a government entity;

(E) in the case of the transfer of a password, the transfer is necessary to use a designated password manager or is to a covered entity for the exclusive purpose of identifying passwords that are being reused across sites or accounts;

(F) in the case of the transfer of genetic information, the transfer is necessary to perform a medical diagnosis or medical treatment specifically requested by an individual, or to conduct medical research in accordance with subsection (a)(2)(J); or

(G) to transfer assets in the manner described in subsection (a)(2)(M); or

(6) in the case of a provider of broadcast television service, cable service, satellite service, streaming media service, or other video programming service described in section 713(h)(2) of the Communications Act of 1934 ([47 U.S.C. 613\(h\)\(2\)](#)), transfer to an unaffiliated third party covered data that reveals the video content or services requested or selected by an individual from such service, except with the affirmative express consent of the individual or pursuant to one of the permissible purposes enumerated in subsection (a)(2)(A) through (O).

(c) Privacy by design.—

(1) Policies, practices, and procedures.—A covered entity and a service provider shall establish, implement, and maintain reasonable policies, practices, and procedures that reflect the role of the covered entity or service provider in the collection, processing, and transferring of covered data and that—

(A) consider applicable Federal laws, rules, or regulations related to covered data the covered entity or service provider collects, processes, or transfers;

(B) identify, assess, and mitigate privacy risks related to covered minors (including, if applicable, with respect to a covered entity that is not an entity meeting the requirements of section 563(e)(2), in a manner that considers the developmental needs of different age ranges of covered minors) to result in reasonably necessary and proportionate residual risk to covered minors;

(C) mitigate privacy risks, including substantial privacy risks, related to the products and services of the covered entity or the service provider, including in the design, development, and implementation of such products and services, taking into account the role of the covered entity or service provider and the information available to it; and

(D) implement reasonable training and safeguards within the covered entity and service provider to promote compliance with all privacy laws applicable to covered data the covered entity collects, processes, or transfers or covered data the service provider collects, processes, or transfers on behalf of the covered entity and mitigate privacy risks, including substantial privacy risks, taking into account the role of the covered entity or service provider and the information available to it.

(2) Factors to consider.—The policies, practices, and procedures established under paragraph (1) shall correspond with, as applicable—

(A) the size of the covered entity or the service provider and the nature, scope, and complexity of the activities engaged in by the covered entity or service provider, including whether the covered entity or service provider is a large data holder, nonprofit organization, entity meeting the requirements of section 563(e)(2), third party, or third-party collecting entity, taking into account the role of the covered entity or service provider and the information available to it;

(B) the sensitivity of the covered data collected, processed, or transferred by the covered entity or service provider;

(C) the volume of covered data collected, processed, or transferred by the covered entity or service provider;

(D) the number of individuals and devices to which the covered data collected, processed, or transferred by the covered entity or service provider relates; and

(E) the cost of implementing such policies, practices, and procedures in relation to the risks and nature of the covered data.

(3) Commission guidance.—Not later than 1 year after the date of enactment of this subtitle, the Commission shall issue guidance as to what constitutes reasonable policies, practices, and

procedures as required by this subsection. The Commission shall consider unique circumstances applicable to nonprofit organizations, to entities meeting the requirements of section 563(e)(2), and to service providers.

(d) Loyalty with respect to pricing.—

(1) Retaliation prohibited.—A covered entity may not retaliate against an individual for exercising any of the protections established by this subtitle, or any regulations promulgated under this subtitle, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services.

(2) Rules of construction.—Nothing in paragraph (1) may be construed to—

(A) prohibit the relation of the price of a service or the level of service provided to an individual to the provision, by the individual, of financial information that is necessarily collected and processed only for the purpose of initiating, rendering, billing for, or collecting payment for a service or product requested by the individual;

(B) prohibit a covered entity from offering a different price, rate, level, quality or selection of goods or services to an individual, including offering goods or services for no fee, if—

(i) the offering is in connection with an individual's voluntary participation in a bona fide loyalty program; and

(ii) the covered entity does not collect, process, or transfer covered data beyond what is strictly necessary to administer such loyalty program;

(C) require a covered entity to provide a bona fide loyalty program that would require the covered entity to collect, process, or transfer covered data that the covered entity otherwise would not collect, process, or transfer;

(D) prohibit a covered entity from offering a financial incentive or other consideration to an individual for participation in market research;

(E) prohibit a covered entity from offering different types of pricing or functionalities with respect to a product or service based on an individual's exercise of a privilege under section 563(c)(1)(C); or

(F) prohibit a covered entity from declining to provide a product or service insofar as the collection and processing of covered data is strictly necessary for such product or service.

(3) Bona fide loyalty program defined.—For purposes of this subsection, the term "bona fide loyalty program" includes rewards, premium features, discount or club card programs.

SEC. 563. CONSUMER DATA CONTROLS.

(a) Consumer awareness.—

(1) In general.—Not later than 120 days after enactment of this Act, the Commission shall publish, on the public website of the Commission, a webpage that describes each provision, protection, obligation, and requirement of this subtitle, listed separately for individuals and for

covered entities and service providers, and the remedies, exemptions, and protections associated with this subtitle, in plain and concise language and in an easy-to-understand manner.

(2) Updates.—The Commission shall update the information published under paragraph (1) on a quarterly basis as necessitated by any change in law, regulation, guidance, or judicial decisions.

(3) Accessibility.—The Commission shall publish the information required to be published under paragraph (1) in the 10 languages with the most users in the United States, according to the most recent United States Census.

(b) Transparency.—

(1) In general.—Each covered entity shall make publicly available, in a clear, conspicuous, not misleading, and easy-to-read and readily accessible manner, a privacy policy that provides a detailed and accurate representation of the data collection, processing, and transfer activities of the covered entity.

(2) Content of privacy policy.—A covered entity or service provider shall have a privacy policy that includes, at a minimum, the following:

(A) The identity and the contact information of—

(i) the covered entity or service provider to which the privacy policy applies (including the covered entity's or service provider's points of contact and generic electronic mail addresses, as applicable for privacy and data security inquiries); and

(ii) any other entity within the same corporate structure as the covered entity or service provider to which covered data is transferred by the covered entity.

(B) The categories of covered data the covered entity or service provider collects or processes.

(C) The processing purposes for each category of covered data the covered entity or service provider collects or processes.

(D) Whether the covered entity or service provider transfers covered data and, if so—

(i) each category of service provider and third party to which the covered entity or service provider transfers covered data;

(ii) the name of each third-party collecting entity to which the covered entity or service provider transfers covered data; and

(iii) the purposes for which such data is transferred to such categories of service providers and third parties or third-party collecting entities.

(E) The length of time the covered entity or service provider intends to retain each category of covered data, including sensitive covered data, including, where practicable, the exact date or dates on which the covered entity or service provider expects to delete or de-identify each such category of covered data, or, if it is not possible to identify that

timeframe or exact date, the criteria used to determine the length of time the covered entity or service provider intends to retain categories of covered data.

(F) A prominent description of how an individual can exercise the privileges and protections established under this subtitle.

(G) A general description of the covered entity's or service provider's data security practices.

(H) The effective date of the privacy policy.

(3) Languages.—The privacy policy required under paragraph (1) shall be made available to the public in each covered language in which the covered entity or service provider—

(A) provides a product or service that is subject to the privacy policy; or

(B) carries out activities related to such product or service.

(4) Accessibility.—The covered entity or service provider shall also provide the disclosures under this subsection in a manner that is reasonably accessible to and usable by individuals with disabilities.

(5) Material changes.—

(A) Affirmative express consent.—If a covered entity makes a material change to its privacy policy or practices, the covered entity shall notify each individual affected by such material change before implementing the material change with respect to any prospectively collected covered data and, except as provided in subparagraphs (A) through (O) of section 562(a)(2), provide a reasonable opportunity for each individual to withdraw consent to any further materially different collection, processing, or transfer of previously collected covered data under the changed policy.

(B) Notification.—The covered entity shall take all reasonable electronic measures to provide direct notification regarding material changes to the privacy policy to each affected individual, in each covered language in which the privacy policy is made available, and taking into account available technology and the nature of the relationship.

(C) Clarification.—Nothing in this paragraph may be construed to affect the requirements for covered entities under section 562(b) or subsection (d).

(D) Log of material changes.—Each large data holder shall retain copies of previous versions of its privacy policy for at least 10 years beginning after the date of enactment of this subtitle and publish all such prior versions, together with a log of material changes, on a dedicated, publicly accessible webpage on its website. Such large data holder shall make publicly available, in a clear, conspicuous, and readily accessible manner, a log describing the date and nature of each material change to its privacy policy over the past 10 years. The descriptions shall be sufficient for a reasonable individual to understand the material effect of each material change. The obligations in this subparagraph shall not apply to any previous versions of a large data holder's privacy policy, or any material changes to such policy, that precede the date of enactment of this subtitle.

(6) Short-form notice to consumers by large data holders.—

(A) In general.—In addition to the privacy policy required under paragraph (1), a large data holder that is a covered entity shall provide a short-form notice of its covered data practices in a manner that is—

(i) concise, clear, conspicuous, and not misleading;

(ii) readily accessible to the individual, based on what is reasonably anticipated within the context of the relationship between the individual and the large data holder;

(iii) inclusive of an overview of individual privileges, protections, and disclosures to reasonably draw attention to data practices that may reasonably be unexpected to a reasonable person or that involve sensitive covered data, including whether covered data will be processed for purposes of algorithmic recommendation systems; and

(iv) no more than 500 words in length.

(B) Rulemaking.—The Commission shall issue a rule pursuant to [section 553 of title 5](#), United States Code, establishing the minimum data disclosures necessary for the short-form notice required under subparagraph (A), which shall not exceed the content requirements in paragraph (2) and shall include templates or models of short-form notices.

(c) Control of data by individuals.—

(1) Access to, and correction, deletion, and portability of, covered data.—In accordance with paragraphs (2) and (3), a covered entity shall provide an individual, after receiving a verified request from the individual, with the ability to—

(A) access—

(i) in a human-readable format that a reasonable individual can understand and download from the internet, the covered data (except covered data in a backup or archival system) of the individual making the request that is collected, processed, or transferred by the covered entity or any service provider of the covered entity within the 24 months preceding the request;

(ii) the categories—

(I) of any service providers to whom the covered entity has sold, or transferred for any consideration, the covered data of the individual;

(II) of sources from which the covered data was collected; and

(III) of any third party to which the covered entity transferred the covered data and, if applicable, an option to obtain the names of those third parties; and

(iii) a description of the purpose for which the covered entity transferred the covered data of the individual to a third party or service provider;

(B) correct any verifiable substantial inaccuracy or substantially incomplete information with respect to the covered data of the individual that is processed by the covered entity

and instruct the covered entity to make reasonable efforts to notify all third parties or service providers to which the covered entity transferred such covered data of the corrected information;

(C) delete covered data of the individual that is processed by the covered entity and instruct the covered entity to make reasonable efforts to notify all third parties or service providers to which the covered entity transferred such covered data of the individual's deletion request;

(D) to the extent technically feasible, export to the individual or directly to another entity the covered data of the individual that is processed by the covered entity, including inferences linked or reasonably linkable to the individual but not including other derived data, without licensing restrictions that limit such transfers in—

(i) a human-readable format that a reasonable individual can understand and download from the internet; and

(ii) a portable, structured, interoperable, and machine-readable format;

(E) disable or opt out of the use of a covered algorithm to rank, order, promote, recommend, amplify, or similarly determine the delivery or display of information to the individual, unless such use is strictly necessary to provide a specific product or service expressly requested by the individual; and

(F) restrict the collection, processing, or transfer of precise geolocation information of the individual and receive clear and conspicuous notice whenever precise geolocation information of the individual is being collected, processed, or transferred.

(2) Individual autonomy.—A covered entity may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of a privilege described in paragraph (1) through—

(A) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(B) the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to exercise such privilege.

(3) Timing.—

(A) In general.—Subject to paragraphs (4) and (5), each request under paragraph (1) shall be completed by any—

(i) large data holder within 45 days of such request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual;

(ii) covered entity that is neither a large data holder nor a covered entity meeting the requirements of subsection (e)(2) within 60 days of such request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual; or

(iii) covered entity meeting the requirements of subsection (e)(2) within 90 days of such request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual.

(B) Extension.—A response period set forth in this paragraph may be extended once by 45 additional days when reasonably necessary, considering the complexity and number of the individual's requests, so long as the covered entity informs the individual of any such extension within the initial 45-day response period, together with the reason for the extension.

(4) Frequency and cost of access.—A covered entity—

(A) shall provide an individual with the opportunity to exercise each of the privileges described in paragraph (1); and

(B) with respect to—

(i) the first 2 times that an individual exercises any privilege described in paragraph (1) in any 12-month period, shall allow the individual to exercise such privilege free of charge; and

(ii) any time beyond the initial 2 times described in clause (i), may allow the individual to exercise such privilege for a reasonable fee for each request.

(5) Verification and exceptions.—

(A) Required exceptions.—A covered entity may not permit an individual to exercise a privilege described in paragraph (1), in whole or in part, if the covered entity—

(i) cannot reasonably verify that the individual making the request to exercise the privilege is the individual whose covered data is the subject of the request or an individual authorized to make such a request on the individual's behalf;

(ii) reasonably believes that the request is made to interfere with a contract between the covered entity and another individual;

(iii) determines that the exercise of the privilege would require access to or correction of another individual's sensitive covered data;

(iv) reasonably believes that the exercise of the privilege would require the covered entity to engage in an unfair, deceptive, or abusive practice under section 5 of the Federal Trade Commission Act ([15 U.S.C. 45](#)); or

(v) reasonably believes that the request is made to further fraud, support criminal activity, or the exercise of the privilege presents a data security threat.

(B) Additional information.—If a covered entity cannot reasonably verify that a request to exercise a privilege described in paragraph (1) is made by the individual whose covered data is the subject of the request (or an individual authorized to make such a request on the individual's behalf), the covered entity—

(i) may request that the individual making the request to exercise the privilege provide any additional information necessary for the sole purpose of verifying the identity of the individual; and

(ii) may not process or transfer such additional information for any other purpose.

(C) Permissive exceptions.—

(i) In general.—A covered entity may decline, with adequate explanation to the individual, to comply with a request to exercise a privilege described in paragraph (1), in whole or in part, that would—

(I) require the covered entity to retain any covered data collected for a single, one-time transaction, if such covered data is not processed or transferred by the covered entity for any purpose other than completing such transaction;

(II) be demonstrably impracticable or prohibitively costly to comply with, and the covered entity shall provide a description to the requestor detailing the inability to comply with the request;

(III) require the covered entity to attempt to re-identify de-identified data;

(IV) require the covered entity to maintain covered data in an identifiable form or collect, retain, or access any data in order to be capable of associating a verified individual request with covered data of such individual;

(V) result in the release of trade secrets or other privileged or confidential business information;

(VI) require the covered entity to correct any covered data that cannot be reasonably verified as being inaccurate or incomplete;

(VII) interfere with law enforcement, judicial proceedings, investigations, or reasonable efforts to guard against, detect, prevent, or investigate fraudulent, malicious, or unlawful activity, or enforce valid contracts;

(VIII) violate Federal or State law or the rights and freedoms of another individual, including under the Constitution of the United States;

(IX) prevent a covered entity from being able to maintain a confidential record of deletion requests, maintained solely for the purpose of preventing covered data of an individual from being recollected after the individual submitted a deletion request and requested that the covered entity no longer collect, process, or transfer such data;

(X) fall within an exception enumerated in the regulations promulgated by the Commission pursuant to clause (iv); or

(XI) with respect to requests for deletion—

(aa) unreasonably interfere with the provision of products or services by the covered entity to another person it currently serves;

(bb) delete covered data that relates to a public figure and for which the requesting individual has no reasonable expectation of privacy;

(cc) delete covered data reasonably necessary to perform a contract between the covered entity and the individual;

(dd) delete covered data that the covered entity needs to retain in order to comply with professional ethical obligations;

(ee) delete covered data that the covered entity reasonably believes may be evidence of unlawful activity or an abuse of the covered entity's products or services; or

(ff) for private elementary and secondary schools as defined by State law and private institutions of higher education as defined by [title I](#) of the Higher Education Act of 1965, delete covered data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution.

(ii) Partial compliance.—In a circumstance that would allow a denial pursuant to clause (i), a covered entity shall partially comply with the remainder of the request if it is possible and not unduly burdensome to do so.

(iii) Number of requests.—For purposes of clause (i)(II), the receipt of a large number of verified requests, on its own, may not be considered to render compliance with a request demonstrably impracticable.

(iv) Further exceptions.—The Commission may, by regulation as described in paragraph (7), establish additional permissive exceptions necessary to protect individual privacy and autonomy, alleviate undue burdens on covered entities, prevent unjust or unreasonable outcomes from the exercise of access, correction, deletion, or portability controls, or as otherwise necessary to fulfill the purposes of this subsection. In establishing such exceptions, the Commission should consider any relevant changes in technology, means for protecting privacy and other legal protections, and beneficial uses of covered data by covered entities.

(6) Large data holder metrics reporting.—A large data holder that is a covered entity shall, for each calendar year in which it was a large data holder, do the following:

(A) Compile the following metrics for the prior calendar year:

(i) The number of verified access requests under paragraph (1)(A).

(ii) The number of verified deletion requests under paragraph (1)(C).

(iii) The number of verified requests under paragraph (1)(E).

(iv) The number of verified requests under paragraph (1)(F).

(v) The number of requests in each of clauses (i) through (iv) that such large data holder complied with in whole or in part and denied.

(vi) The median or mean number of days within which such large data holder substantively responded to the requests in each of clauses (i) through (iv).

(B) Disclose by July 1 of each applicable calendar year the information compiled in subparagraph (A) within such large data holder's privacy policy required under subsection (b) or on the publicly accessible website of such large data holder that is accessible from a hyperlink included in the privacy policy.

(7) Interim final rules.—Not later than 180 days after the date of enactment of this Act, the Commission shall issue interim final rules as necessary to establish processes by which covered entities are to comply with this subsection. The interim final rules shall take effect upon publication in the Federal Register, shall have the force and effect of law, and may be issued without regard to [section 553 of title 5](#), United States Code. The Commission shall provide a public comment period of not less than 60 days after publication and shall issue final rules not later than 18 months after the date of enactment of this Act. Such rules shall take into consideration—

(A) the size of, and the nature, scope, and complexity of the activities engaged in by the covered entity, including whether the covered entity is a large data holder, nonprofit organization, covered entity meeting the requirements of subsection (e)(2), third party, or third-party collecting entity;

(B) the sensitivity of covered data collected, processed, or transferred by the covered entity;

(C) the volume of covered data collected, processed, or transferred by the covered entity;

(D) the number of individuals and devices to which the covered data collected, processed, or transferred by the covered entity relates; and

(E) after consulting the National Institute of Standards and Technology, standards for ensuring the deletion of covered data under this subtitle where appropriate.

(8) Applicability.—Paragraphs (1) through (6) shall apply beginning on the date that is 180 days after the date of enactment of this Act.

(9) Accessibility.—A covered entity shall facilitate the ability of individuals to make requests under paragraph (1) in any covered language in which the covered entity provides a product or service. The mechanisms by which a covered entity enables individuals to make requests under paragraph (1) shall be readily accessible and usable by individuals with disabilities.

(d) Privacy by default.—

(1) Privacy by default.—It shall be unlawful for a covered entity or service provider to configure any privacy setting or option made available to an individual, with respect to the collection, processing, or transfer of covered data, to default to any such setting or option other than the most privacy-protective setting offered by such covered entity or service provider.

(2) Opt-in required for reduced privacy.—It shall be unlawful for a covered entity or service provider to apply a less protective privacy setting to an individual unless such individual has provided affirmative express consent.

(3) Targeted advertising.—It shall be unlawful for a covered entity or service provider to engage in targeted advertising, except for the dissemination of an advertisement targeted exclusively on a recognized place in accordance with section 567(b)(3).

(4) Withdrawal of consent.—A covered entity shall provide an individual with a clear and conspicuous, easy-to-execute means to withdraw any affirmative express consent previously provided by the individual that is as easy to execute by a reasonable individual as the means to provide consent.

(5) Individual autonomy.—A covered entity may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of any individual protection under this subsection through—

(A) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(B) the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to exercise any such protection.

(e) Small business protections.—

(1) Establishment of exemption.—Any covered entity or service provider that can establish that it met the requirements described in paragraph (2) for the period of the 3 preceding calendar years (or for the period during which the covered entity or service provider has been in existence if such period is less than 3 years) shall—

(A) be exempt from compliance with subparagraph (D) of subsection (c)(1), subparagraphs (A) through (C) and (E) through (G) of section 564(a)(2), and section 565(a)(3); and

(B) at the covered entity's sole discretion, have the option of complying with subsection (c)(1)(B) by, after receiving a verified request from an individual to correct covered data of the individual under such subparagraph, deleting such covered data in its entirety instead of making the requested correction.

(2) Exemption requirements.—The requirements of this paragraph are, with respect to a covered entity or a service provider, the following:

(A) The covered entity or service provider's average annual gross revenues during the period did not exceed \$41,000,000.

(B) The covered entity or service provider, on average, did not annually collect or process the covered data of more than 200,000 individuals during the period beyond the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product, so long as all covered data for such purpose

was deleted or de-identified within 90 days, except when necessary to investigate fraud or as consistent with a covered entity's return policy.

(C) The covered entity or service provider did not derive more than 50 percent of its revenue from transferring covered data during any year (or part of a year if the covered entity has been in existence for less than 1 year) that occurs during the period.

(3) Revenue defined.—For purposes of this subsection, the term "revenue" as it relates to any covered entity or service provider that is not organized to carry on business for its own profit or that of its members, means the gross receipts the covered entity or service provider received in whatever form from all sources without subtracting any costs or expenses, and includes contributions, gifts, grants, dues or other assessments, income from investments, or proceeds from the sale of real or personal property.

(f) Unified privacy mechanisms.—

(1) In general.—For the protections established under subsection (d), for the communication of a refusal or withdrawal of consent for a transfer of covered data to a third party that is not strictly necessary to provide, maintain, complete, or fulfill a specific product or service requested by the individual, and for requests under section 564(b)(2)(C)(iii), following public notice and opportunity to comment and not later than January 1, 2028, the Commission shall establish or recognize 1 or more acceptable privacy-protective, centralized mechanisms, including browser or device privacy settings, other tools offered by covered entities or service providers, and registries of identifiers, for individuals to exercise all such protections through a single interface for a covered entity or service provider to utilize.

(2) Requirements.—Any such centralized mechanism shall—

(A) require covered entities or service providers acting on behalf of covered entities to inform individuals about the mechanism and its effect;

(B) operate as the default privacy-protective setting unless the individual affirmatively chooses a different setting, and any such different setting shall clearly represent the individual's affirmative, freely given, specific, and unambiguous choice;

(C) be consumer-friendly, clearly described, and easy-to-use by a reasonable individual;

(D) permit the covered entity or service provider acting on behalf of a covered entity to have an authentication process the covered entity or service provider acting on behalf of a covered entity may use to determine if the mechanism represents a legitimate request;

(E) be provided in any covered language in which the covered entity provides products or services subject to the mechanism; and

(F) be provided in a manner that is reasonably accessible to and usable by individuals with disabilities.

SEC. 564. DATA SECURITY AND REGISTRATION.

(a) Data security and protection of covered data.—

(1) Establishment of data security practices.—

(A) In general.—A covered entity or service provider shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices and procedures to protect and secure covered data against unauthorized access and acquisition.

(B) Considerations.—The reasonable administrative, technical, and physical data security practices required under subparagraph (A) shall be appropriate to—

- (i) the size and complexity of the covered entity or service provider;
- (ii) the nature and scope of the covered entity or the service provider's collecting, processing, or transferring of covered data;
- (iii) the volume and nature of the covered data collected, processed, or transferred by the covered entity or service provider;
- (iv) the sensitivity of the covered data collected, processed, or transferred;
- (v) the current state of the art (and limitations thereof) in administrative, technical, and physical safeguards for protecting such covered data; and
- (vi) the cost of available tools to improve security and reduce vulnerabilities to unauthorized access and acquisition of such covered data in relation to the risks and nature of the covered data.

(2) Specific requirements.—The data security practices of the covered entity and of the service provider required under paragraph (1) shall include, for each respective entity's own system or systems, at a minimum, the following practices:

(A) Assess vulnerabilities.—Identifying and assessing any material internal and external risk to, and vulnerability in, the security of each system maintained by the covered entity that collects, processes, or transfers covered data, or service provider that collects, processes, or transfers covered data on behalf of the covered entity, including unauthorized access to or risks to such covered data, human vulnerabilities, access rights, and the use of service providers. With respect to large data holders, such activities shall include a plan to receive and reasonably respond to unsolicited reports of vulnerabilities by any entity or individual and to perform a reasonable investigation of such reports.

(B) Preventive and corrective action.—Taking preventive and corrective action designed to mitigate reasonably foreseeable risks or vulnerabilities to covered data identified by the covered entity or service provider, consistent with the nature of such risk or vulnerability and the entity's role in collecting, processing, or transferring the data. Such action may include implementing administrative, technical, or physical safeguards or changes to data security practices or the architecture, installation, or implementation of network or operating software, among other actions.

(C) Evaluation of preventive and corrective action.—Evaluating and making reasonable adjustments to the action described in subparagraph (B) in light of any material changes in

technology, internal or external threats to covered data, and the covered entity or service provider's own changing business arrangements or operations.

(D) Information retention and disposal.—Disposing of covered data in accordance with a retention schedule that shall require the deletion of covered data when such data is required to be deleted by law or is no longer necessary for the purpose for which the data was collected, processed, or transferred, unless an individual has provided affirmative express consent to such retention. Such disposal shall include destroying, permanently erasing, or otherwise modifying the covered data to make such data permanently unreadable or indecipherable and unrecoverable to ensure ongoing compliance with this subsection. Service providers shall establish practices to delete or return covered data to a covered entity as requested at the end of the provision of services unless retention of the covered data is required by law, consistent with section 565(b)(1)(F).

(E) Training.—Training each employee with access to covered data on how to safeguard covered data and updating such training as necessary.

(F) Designation.—Designating an officer, employee, or employees to maintain and implement such practices.

(G) Incident response.—Implementing procedures to detect, respond to, or recover from security incidents, including breaches.

(3) Regulations.—The Commission may promulgate, in accordance with [section 553 of title 5](#), United States Code, technology-neutral regulations to establish processes for complying with this subsection. The Commission shall consult with the National Institute of Standards and Technology in establishing such processes.

(b) Third-party collecting entities.—

(1) Notice.—Each third-party collecting entity shall place a clear, conspicuous, not misleading, and readily accessible notice on the website or mobile application of the third-party collecting entity (if the third-party collecting entity maintains such a website or mobile application) that—

(A) notifies individuals that the entity is a third-party collecting entity using specific language that the Commission shall develop through rulemaking under [section 553 of title 5](#), United States Code, except that, until such language takes effect, language clearly and conspicuously identifying the entity as a third-party collecting entity shall satisfy this subparagraph;

(B) includes a link to the website established under paragraph (2)(C); and

(C) is reasonably accessible to and usable by individuals with disabilities.

(2) Third-party collecting entity registration.—

(A) In general.—Not later than January 31 of each calendar year that follows a calendar year during which a covered entity acted as a third-party collecting entity and processed covered data pertaining to more than 5,000 individuals or devices that identify or are linked

or reasonably linkable to an individual, such covered entity shall register with the Commission in accordance with this subsection.

(B) Registration requirements.—In registering with the Commission as required under subparagraph (A), a third-party collecting entity shall do the following:

(i) Pay to the Commission a registration fee of \$100.

(ii) Provide the Commission with the following information:

(I) The legal name and primary physical, email, and internet addresses of the third-party collecting entity.

(II) A description of the categories of covered data the third-party collecting entity processes and transfers.

(III) The contact information of the third-party collecting entity, including a contact person, a telephone number, an email address, a website, and a physical mailing address.

(IV) A link to a website through which an individual may easily exercise the rights provided under this subsection.

(C) Third-party collecting entity registry.—The Commission shall establish and maintain on a website a searchable, publicly available, central registry of third-party collecting entities that are registered with the Commission under this subsection that includes the following:

(i) A listing of all registered third-party collecting entities and a search feature that allows members of the public to identify individual third-party collecting entities.

(ii) For each registered third-party collecting entity, the information provided under subparagraph (B).

(iii) (I) A "Do Not Collect" registry link and mechanism by which an individual may easily submit a request to all registered third-party collecting entities that are not consumer reporting agencies (as defined in section 603(f) of the Fair Credit Reporting Act ([15 U.S.C. 1681a\(f\)](#))), and to the extent such third-party collecting entities are not acting as consumer reporting agencies (as so defined), to—

(aa) delete all covered data related to such individual that the third-party collecting entity did not collect from such individual directly or when acting as a service provider; and

(bb) ensure that the third-party collecting entity no longer collects covered data related to such individual without the affirmative express consent of such individual, except insofar as the third-party collecting entity is acting as a service provider.

(II) Each third-party collecting entity that receives such a request from an individual shall delete all covered data described in subclause (I)(aa) relating to the

individual not later than 30 days after the request is received by the third-party collecting entity.

(III) Notwithstanding subclauses (I) and (II), a third-party collecting entity may decline to fulfill a "Do Not Collect" request from an individual who it has actual knowledge has been convicted of a crime related to the abduction or sexual exploitation of a child, and the data the entity is collecting is necessary to effectuate the purposes of a national or State-run sex offender registry or the congressionally designated entity that serves as the nonprofit national resource center and clearinghouse to provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children issues.

(3) Penalties.—

(A) In general.—A third-party collecting entity that fails to register or provide the notice as required under this subsection shall be liable for—

(i) a civil penalty of \$5,000 for each day the third-party collecting entity fails to register or provide notice as required under this subsection, not to exceed a total of \$500,000 for any year; and

(ii) an amount equal to the registration fees due under paragraph (2)(B)(i) for each year that the third-party collecting entity failed to register as required.

(B) Rule of construction.—Nothing in this paragraph shall be construed as altering, limiting, or affecting any enforcement authorities or remedies under this subtitle.

(c) Civil rights and algorithms.—

(1) Civil rights protections.—

(A) In general.—A covered entity or a service provider may not collect, process, or transfer covered data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability.

(B) Exceptions.—This paragraph shall not apply to—

(i) the collection, processing, or transfer of covered data for the purpose of self-testing to prevent or mitigate unlawful discrimination; or

(ii) any private club or group not open to the public, as described in section 201(e) of the Civil Rights Act of 1964 ([42 U.S.C. 2000a\(e\)](#)).

(2) FTC enforcement assistance.—

(A) In general.—Whenever the Commission obtains information that a covered entity or service provider may have collected, processed, or transferred covered data in violation of paragraph (1), the Commission shall transmit such information as allowable under Federal law to any Executive agency with authority to initiate enforcement actions or proceedings relating to such violation.

(B) Annual report.—Not later than 3 years after the date of enactment of this subtitle, and annually thereafter, the Commission shall submit to Congress a report that includes a summary of—

(i) the types of information the Commission transmitted to Executive agencies under subparagraph (A) during the previous 1-year period; and

(ii) how such information relates to Federal civil rights laws.

(C) Technical assistance.—In transmitting information under subparagraph (A), the Commission may consult and coordinate with, and provide technical and investigative assistance, as appropriate, to such Executive agency.

(D) Cooperation with other agencies.—The Commission may implement this paragraph by executing agreements or memoranda of understanding with the appropriate Executive agencies.

(3) Covered algorithm impact and evaluation.—

(A) Covered algorithm impact assessment.—

(i) Impact assessment.—Notwithstanding any other provision of law, not later than July 1, 2028, and annually thereafter, a large data holder that uses a covered algorithm in a manner that poses a consequential risk of harm to an individual or group of individuals, and uses such covered algorithm solely or in part, to collect, process, or transfer covered data shall conduct an impact assessment of such algorithm in accordance with clause (ii).

(ii) Impact assessment scope.—The impact assessment required under clause (i) shall provide the following:

(I) A detailed description of the design process and methodologies of the covered algorithm.

(II) A statement of the purpose and proposed uses of the covered algorithm.

(III) A detailed description of the data used by the covered algorithm, including the specific categories of data that will be processed as input and any data used to train the model that the covered algorithm relies on, if applicable.

(IV) A description of the outputs produced by the covered algorithm.

(V) An assessment of the necessity and proportionality of the covered algorithm in relation to its stated purpose.

(VI) A detailed description of steps the large data holder has taken or will take to mitigate potential harms from the covered algorithm to an individual or group of individuals, including related to—

(aa) covered minors;

(bb) making or facilitating advertising for, or determining access to, or restrictions on the use of housing, education, employment, health care, insurance, or credit opportunities;

(cc) determining access to, or restrictions on the use of, any place of public accommodation, particularly as such harms relate to the protected characteristics of individuals, including race, color, religion, national origin, sex, or disability;

(dd) disparate impact on the basis of individuals' race, color, religion, national origin, sex, or disability status; or

(ee) disparate impact on the basis of individuals' political party registration status.

(B) Algorithm design evaluation.—Notwithstanding any other provision of law, not later than 2 years after the date of enactment of this subtitle, a covered entity or service provider that knowingly develops a covered algorithm that is designed, solely or in part, to collect, process, or transfer covered data in furtherance of a consequential decision shall prior to deploying the covered algorithm in interstate commerce evaluate the design, structure, and inputs of the covered algorithm, including any training data used to develop the covered algorithm, to reduce the risk of the potential harms identified under subparagraph (A)(ii).

(C) Other considerations.—

(i) Focus.—In complying with subparagraphs (A) and (B), a covered entity and a service provider may focus the impact assessment or evaluation on any covered algorithm, or portions of a covered algorithm, that will be put to use and may reasonably contribute to the risk of the potential harms identified under subparagraph (A)(ii).

(ii) Availability.—

(I) In general.—A covered entity and a service provider—

(aa) shall, not later than 30 days after completing an impact assessment or evaluation, submit the impact assessment or evaluation conducted under subparagraph (A) or (B) to the Commission;

(bb) shall, upon request, make such impact assessment and evaluation available to Congress; and

(cc) may make a summary of such impact assessment and evaluation publicly available in a place that is easily accessible to individuals.

(II) Trade secrets.—Covered entities and service providers may redact and segregate any trade secret (as defined in [section 1839 of title 18](#), United States Code) or other confidential or proprietary information from public disclosure under this clause and the Commission shall abide by its obligations under section 6(f) of the Federal Trade Commission Act ([15 U.S.C. 46\(f\)](#)) in regard to such information.

(iii) Enforcement.—The Commission may not use any information obtained solely and exclusively through a covered entity or a service provider's disclosure of information to the Commission in compliance with this paragraph for any purpose other than enforcing this subtitle with the exception of enforcing consent orders, including the study and report provisions in subparagraph (F). This clause does not preclude the Commission from providing this information to Congress in response to a subpoena.

(D) Guidance.—Not later than 2 years after the date of enactment of this subtitle, the Commission shall, in consultation with the Secretary of Commerce or their designee, publish guidance regarding compliance with this paragraph.

(E) Rulemaking and exemption.—The Commission shall have authority under [section 553 of title 5](#), United States Code, to promulgate regulations as necessary to establish processes by which a large data holder—

(i) shall submit an impact assessment to the Commission under clause (ii)(I) of subparagraph (C); and

(ii) may exclude from this paragraph any covered algorithm that presents low or minimal consequential risk of harm to an individual or group of individuals.

(F) Study and report.—

(i) Study.—The Commission, in consultation with the Secretary of Commerce or the Secretary's designee, shall conduct a study, to review any impact assessment or evaluation submitted under this paragraph. Such study shall include an examination of—

(I) best practices for the assessment and evaluation of covered algorithms; and

(II) methods to reduce the risk of harm to individuals that may be related to the use of covered algorithms.

(ii) Report.—

(I) Initial report.—Not later than 3 years after the date of enactment of this subtitle, the Commission, in consultation with the Secretary of Commerce or the Secretary's designee, shall submit to Congress a report containing the results of the study conducted under subclause (i), together with recommendations for such legislation and administrative action as the Commission determines appropriate.

(II) Additional reports.—Not later than 3 years after submission of the initial report under subclause (I), and as the Commission determines necessary thereafter, the Commission shall submit to Congress an updated version of such report.

(G) Definitions.—In this paragraph:

(i) Consequential decision.—The term "consequential decision" means a decision that determines or materially affects an individual's access to, eligibility for, or terms of housing, education, employment, health care, insurance, credit, or a place of public accommodation.

(ii) Consequential risk of harm.—The term "consequential risk of harm" means a material risk of one or more of the potential harms described in subparagraph (A)(ii).

SEC. 565. EXECUTIVE RESPONSIBILITY, SERVICE PROVIDERS, AND COMPLIANCE PROGRAMS.

(a) Executive responsibility.—

(1) In general.—Beginning 1 year after the date of enactment of this subtitle, an executive officer of a large data holder shall annually certify, in good faith, to the Commission, in a manner specified by the Commission by regulation under [section 553 of title 5](#), United States Code, issued not later than 180 days after the date of enactment of this subtitle, that the entity maintains—

(A) internal controls reasonably designed to comply with this subtitle; and

(B) internal reporting structures to ensure that such certifying executive officer is involved in and responsible for the decisions that impact the compliance by the large data holder with this subtitle.

(2) Requirements.—A certification submitted under paragraph (1) shall be based on a review of the effectiveness of the internal controls and reporting structures of the large data holder that is conducted by the certifying executive officer not more than 90 days before the submission of the certification. A certification submitted under paragraph (1) is made in good faith if the certifying officer had, after a reasonable investigation, reasonable ground to believe and did believe, at the time that certification was submitted, that the statements therein were true and that there was no omission to state a material fact required to be stated therein or necessary to make the statements therein not misleading.

(3) Designation of privacy and data security officer.—

(A) In general.—A covered entity or service provider with more than 15 employees shall designate—

(i) 1 or more qualified employees as privacy officers; and

(ii) 1 or more qualified employees (in addition to any employee designated under clause (i)) as data security officers.

(B) Requirements for officers.—An employee who is designated by a covered entity or a service provider as a privacy officer or a data security officer pursuant to subparagraph (A) shall, at a minimum—

(i) implement a data privacy program and data security program to safeguard the privacy and security of covered data in compliance with the requirements of this subtitle; and

(ii) facilitate the covered entity or service provider's ongoing compliance with this subtitle.

(C) Additional requirements for large data holders.—A large data holder shall designate at least 1 of the officers described in subparagraph (A) to report directly to the highest official at the large data holder as a privacy protection officer who shall, in addition to the requirements in subparagraph (B), either directly or through a supervised designee or designees—

(i) establish processes to periodically review and update the privacy and security policies, practices, and procedures of the large data holder, as necessary;

(ii) conduct biennial and comprehensive audits to ensure the policies, practices, and procedures of the large data holder ensure the large data holder is in compliance with this subtitle and ensure such audits are accessible to the Commission upon request;

(iii) develop a program to educate and train employees about compliance requirements of this subtitle;

(iv) maintain updated, accurate, clear, and understandable records of all material privacy and data security practices undertaken by the large data holder; and

(v) serve as the point of contact between the large data holder and enforcement authorities.

(4) Large data holder privacy impact assessments.—

(A) In general.—Not later than July 1, 2027, or 1 year after the date on which a covered entity first meets the definition of large data holder, and biennially thereafter, each covered entity that is a large data holder shall conduct a privacy impact assessment that weighs the benefits of the large data holder's covered data collecting, processing, and transfer practices against the potential adverse consequences of such practices, including substantial privacy risks, to individual privacy.

(B) Assessment requirements.—A privacy impact assessment required under subparagraph (A) shall be—

(i) reasonable and appropriate in scope given—

(I) the nature of the covered data collected, processed, and transferred by the large data holder;

(II) the volume of the covered data collected, processed, and transferred by the large data holder; and

(III) the potential material risks posed to the privacy of individuals by the collecting, processing, and transfer of covered data by the large data holder;

(ii) documented in written form and maintained by the large data holder unless rendered out of date by a subsequent assessment conducted under subparagraph (A); and

(iii) approved by the privacy protection officer designated under paragraph (3)(C).

(C) Additional factors to include in assessment.—In assessing the privacy risks, including substantial privacy risks, the large data holder must include reviews of the means by which technologies, including blockchain and distributed ledger technologies and other emerging technologies, are used to secure covered data.

(5) Other privacy impact assessments.—

(A) In general.—Not later than 1 year after the date of enactment of this subtitle and biennially thereafter, each covered entity that is not a large data holder and does not meet the requirements for covered entities under section 563(e)(2) shall conduct a privacy impact assessment. Such assessment shall weigh the benefits of the covered entity's covered data collecting, processing, and transfer practices that may cause a substantial privacy risk against the potential material adverse consequences of such practices to individual privacy.

(B) Assessment requirements.—A privacy impact assessment required under subparagraph (A) shall be—

(i) reasonable and appropriate in scope given—

(I) the nature of the covered data collected, processed, and transferred by the covered entity;

(II) the volume of the covered data collected, processed, and transferred by the covered entity; and

(III) the potential risks posed to the privacy of individuals by the collecting, processing, and transfer of covered data by the covered entity; and

(ii) documented in written form and maintained by the covered entity unless rendered out of date by a subsequent assessment conducted under subparagraph (A).

(C) Additional factors to include in assessment.—In assessing the privacy risks, including substantial privacy risks, the covered entity may include reviews of the means by which technologies, including blockchain and distributed ledger technologies and other emerging technologies, are used to secure covered data.

(b) Service providers and third parties.—

(1) Service providers.—A service provider—

(A) shall adhere to the instructions of a covered entity and only collect, process, and transfer service provider data to the extent necessary and proportionate to provide a service requested by the covered entity, as set out in the contract required by paragraph (2), and this subparagraph does not require a service provider to collect, process, or transfer covered data if the service provider would not otherwise do so;

(B) may not collect, process, or transfer service provider data if the service provider has actual knowledge that a covered entity violated this subtitle with respect to such data;

(C) shall assist a covered entity in responding to a request made by an individual under section 563(c), by either—

(i) providing appropriate technical and organizational measures, taking into account the nature of the processing and the information reasonably available to the service provider, for the covered entity to comply with such request for service provider data; or

(ii) fulfilling a request by a covered entity to execute an individual rights request that the covered entity has determined should be complied with, by either—

(I) complying with the request pursuant to the covered entity's instructions; or

(II) providing written verification to the covered entity that it does not hold covered data related to the request, that complying with the request would be inconsistent with its legal obligations, or that the request falls within an exception to section 563(c);

(D) may engage another service provider for purposes of processing service provider data on behalf of a covered entity only after providing that covered entity with notice and pursuant to a written contract that requires such other service provider to satisfy the obligations of the service provider with respect to such service provider data, including that the other service provider be treated as a service provider under this subtitle;

(E) shall, upon the reasonable request of the covered entity, make available to the covered entity information necessary to demonstrate the compliance of the service provider with the requirements of this subtitle, which may include making available a report of an independent assessment arranged by the service provider on terms agreed to by the service provider and the covered entity, providing information necessary to enable the covered entity to conduct and document a privacy impact assessment required under subsection (a), and making available the impact assessment or evaluation required under section 564(c)(3);

(F) shall, at the covered entity's direction, delete or return all covered data to the covered entity as requested at the end of the provision of services, unless retention of the covered data is required by law;

(G) shall develop, implement, and maintain reasonable administrative, technical, and physical safeguards that are designed to protect the security and confidentiality of covered data the service provider processes consistent with section 564(a); and

(H) shall allow and cooperate with reasonable assessments by the covered entity or the covered entity's designated assessor; alternatively, the service provider may arrange for a qualified and independent assessor to conduct an assessment of the service provider's policies and technical and organizational measures in support of the obligations under this subtitle using an appropriate and accepted control standard or framework and assessment procedure for such assessments, and shall provide a report of such assessment to the covered entity upon request.

(2) Contracts between covered entities and service providers.—

(A) Requirements.—A person or entity may only act as a service provider pursuant to a written contract between the covered entity and the service provider, or a written contract

between 1 service provider and a second service provider as described under paragraph (1)(D), if the contract—

- (i) sets forth the data processing procedures of the service provider with respect to collection, processing, or transfer performed on behalf of the covered entity or service provider;

- (ii) clearly sets forth—

- (I) instructions for collecting, processing, or transferring data;

- (II) the nature and purpose of collecting, processing, or transferring;

- (III) the type of data subject to collecting, processing, or transferring;

- (IV) the duration of processing; and

- (V) the rights and obligations of both parties, including a method by which the service provider shall notify the covered entity of material changes to its privacy practices;

- (iii) does not relieve a covered entity or a service provider of any requirement or liability imposed on such covered entity or service provider under this subtitle; and

- (iv) prohibits—

- (I) collecting, processing, or transferring covered data in contravention of paragraph (1); and

- (II) combining service provider data with covered data that the service provider receives from or on behalf of another person or persons or collects from the interaction of the service provider with an individual, unless such combining is necessary to effectuate a purpose described in subparagraphs (A) through (O) of section 562(a)(2) and is otherwise permitted under the contract required by this paragraph.

(B) Contract terms.—Each service provider shall retain copies of previous contracts entered into in compliance with this paragraph with each covered entity to which the service provider provides requested products or services.

(3) Relationship between covered entities and service providers.—

(A) Determination.—Determining whether a person is acting as a covered entity or service provider with respect to a specific processing of covered data is a fact-based determination that depends upon the context in which such data is processed.

(B) Change in role.—A person that is not limited in its processing of covered data pursuant to the instructions of a covered entity, or that fails to adhere to such instructions, is a covered entity and not a service provider with respect to a specific processing of covered data. A service provider that continues to adhere to the instructions of a covered entity with respect to a specific processing of covered data remains a service provider. If a service provider begins, alone or jointly with others, determining the purposes and means of the

processing of covered data, the service provider is a covered entity and not a service provider with respect to the processing of such data.

(C) Transferor liability.—A covered entity that transfers covered data to a service provider, or a service provider that transfers covered data to a covered entity or another service provider, in compliance with the requirements of this subtitle, is not liable for a violation of this subtitle by the service provider or covered entity to whom such covered data was transferred, if at the time of transferring such covered data, the covered entity or service provider did not have actual knowledge that the service provider or covered entity would violate this subtitle.

(D) Recipient liability.—A covered entity or service provider that receives covered data in compliance with the requirements of this subtitle is not in violation of this subtitle as a result of a violation by a covered entity or service provider from which such data was received.

(4) Third parties.—A third party—

(A) shall not process third-party data for a processing purpose other than—

(i) in the case of sensitive covered data, the processing purpose for which the individual gave affirmative express consent or to effect a purpose enumerated in subparagraph (A), (C), or (E) of section 562(a)(2); and

(ii) in the case of non-sensitive covered data, the processing purpose for which the covered entity made a disclosure pursuant to section 563(b)(2)(D); and

(B) for purposes of subparagraph (A), may reasonably rely on representations made by the covered entity that transferred the third-party data if the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible, unless the third party has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such representations are false or incomplete.

(5) Additional obligations.—

(A) In general.—A covered entity or service provider shall exercise reasonable due diligence in—

(i) selecting a service provider; and

(ii) deciding to transfer covered data to a third party.

(B) Guidance.—Not later than July 1, 2027, the Commission shall publish guidance regarding compliance with this paragraph, taking into consideration the burdens on large data holders, covered entities who are not large data holders, and covered entities meeting the requirements of section 563(e).

(6) Rule of construction.—Solely for purposes of this subsection, the requirements for service providers to contract with, assist, and follow the instructions of covered entities shall be read to include requirements to contract with, assist, and follow the instructions of a government entity if the service provider is providing a service to a government entity.

(c) Technical compliance programs.—

(1) In general.—Not later than July 1, 2028, the Commission shall promulgate regulations under [section 553 of title 5, United States Code](#), to establish a process for the proposal and approval of technical compliance programs under this subsection used by a covered entity to collect, process, or transfer covered data.

(2) Scope of programs.—The technical compliance programs established under this subsection shall, with respect to a technology, product, service, or method used by a covered entity to collect, process, or transfer covered data—

(A) establish publicly available guidelines for compliance with this subtitle; and

(B) meet or exceed the requirements of this subtitle.

(3) Approval process.—

(A) In general.—Any request for approval, amendment, or repeal of a technical compliance program may be submitted to the Commission by any person, including a covered entity, a representative of a covered entity, an association of covered entities, or a public interest group or organization. Within 90 days after the request is made, the Commission shall publish the request and provide an opportunity for public comment on the proposal.

(B) Expedited response to requests.—Beginning 1 year after the date of enactment of this subtitle, the Commission shall act upon a request for the proposal and approval of a technical compliance program not later than 1 year after the filing of the request, and shall set forth publicly in writing the conclusions of the Commission with regard to such request.

(4) Judicial review.—Final action by the Commission on a request for approval, amendment, or repeal of a technical compliance program, or the failure to act within the 1-year period after a request for approval, amendment, or repeal of a technical compliance program is made under paragraph (3), may be appealed to a Federal district court of the United States of appropriate jurisdiction as provided for in [section 702 of title 5, United States Code](#).

(5) Effect on enforcement.—

(A) In general.—Prior to commencing an investigation or enforcement action against any covered entity under this subtitle, the Commission and State attorney general shall consider the covered entity's history of compliance with any technical compliance program approved under this subsection and any action taken by the covered entity to remedy noncompliance with such program. If an action described in section 569(b)(3) is brought, the covered entity's history of compliance with any technical compliance program approved under this subsection and any action taken by the covered entity to remedy noncompliance with such program shall be taken into consideration when determining liability or a penalty. The covered entity's history of compliance with any technical compliance program shall not affect any burden of proof or the weight given to evidence in an enforcement or judicial proceeding.

(B) Commission authority.—Approval of a technical compliance program shall not limit the authority of the Commission, including the Commission's authority to commence an investigation or enforcement action against any covered entity under this subtitle or any other Act.

(C) Rule of construction.—Nothing in this paragraph shall entitle any individual, class of individuals, or person to seek discovery of any nonpublic Commission deliberation or activity, and nothing in this paragraph shall impose any pleading requirement on the Commission if the Commission brings an enforcement action of any kind.

(d) Commission-approved compliance guidelines.—

(1) Application for compliance guideline approval.—

(A) In general.—A covered entity that is not a third-party collecting entity and meets the requirements of section 563(e), or a group of such covered entities, may apply to the Commission for approval of 1 or more sets of compliance guidelines governing the collection, processing, and transfer of covered data by the covered entity or group of covered entities.

(B) Application requirements.—Such application shall include—

(i) a description of how the proposed guidelines will meet or exceed the requirements of this subtitle;

(ii) a description of the entities or activities the proposed set of compliance guidelines is designed to cover;

(iii) a list of the covered entities that meet the requirements of section 563(e) and are not third-party collecting entities, if any are known at the time of application, that intend to adhere to the compliance guidelines; and

(iv) a description of how such covered entities will be independently assessed for adherence to such compliance guidelines, including the independent organization not associated with any of the covered entities that may participate in guidelines that will administer such guidelines.

(2) Commission review.—

(A) Initial approval.—

(i) Public comment period.—Within 90 days after the receipt of proposed guidelines submitted pursuant to paragraph (1)(B), the Commission shall publish the application and provide an opportunity for public comment on such compliance guidelines.

(ii) Approval.—The Commission shall approve an application regarding proposed guidelines under paragraph (1)(B) if the applicant demonstrates that the compliance guidelines—

(I) meet or exceed the requirements of this subtitle;

(II) provide for the regular review and validation by an independent organization not associated with any of the covered entities that may participate in the guidelines and that is approved by the Commission to conduct such reviews of the compliance guidelines of the covered entity or entities to ensure that the covered entity or entities continue to meet or exceed the requirements of this subtitle; and

(III) include a means of enforcement if a covered entity does not meet or exceed the requirements in the guidelines, which may include referral to the Commission for enforcement consistent with section 569(b)(1) or referral to the appropriate State attorney general for enforcement consistent with section 569(b)(2).

(iii) Timeline.—Within 1 year after receiving an application regarding proposed guidelines under paragraph (1)(B), the Commission shall issue a determination approving or denying the application and providing its reasons for approving or denying such application.

(B) Approval of modifications.—

(i) In general.—If the independent organization administering a set of guidelines makes material changes to guidelines previously approved by the Commission, the independent organization shall submit the updated guidelines to the Commission for approval. As soon as feasible, the Commission shall publish the updated guidelines and provide an opportunity for public comment.

(ii) Timeline.—The Commission shall approve or deny any material change to the guidelines within 1 year after receipt of the submission for approval.

(3) Withdrawal of approval.—If at any time the Commission determines that the guidelines previously approved no longer meet the requirements of this subtitle or a regulation promulgated under this subtitle or that compliance with the approved guidelines is insufficiently enforced by the independent organization administering the guidelines, the Commission shall notify the covered entities or group of such entities and the independent organization of the determination of the Commission to withdraw approval of such guidelines and the basis for doing so. Within 180 days after receipt of such notice, the covered entity or group of such entities and the independent organization may cure any alleged deficiency with the guidelines or the enforcement of such guidelines and submit each proposed cure to the Commission. If the Commission determines that such cures eliminate the alleged deficiency in the guidelines, the Commission may not withdraw approval of such guidelines on the basis of such determination.

(4) Deemed compliance.—A covered entity that is eligible to participate under paragraph (1)(A) and participates in guidelines approved under this subsection shall be deemed in compliance with the relevant provisions of this subtitle if such covered entity is in compliance with such guidelines.

(e) Bureau of Privacy.—

(1) In general.—The Commission shall establish within the Commission a new bureau to be known as the "Bureau of Privacy", which shall be of similar structure, size, organization, and

authority as the existing bureaus within the Commission related to consumer protection and competition.

(2) Mission.—The mission of the Bureau established under paragraph (1) shall be to assist the Commission in carrying out the duties of the Commission under this subtitle and related duties under other provisions of law.

(3) Timeline.—The Bureau required to be established under paragraph (1) shall be established, staffed, and fully operational not later than 1 year after the date of enactment of this subtitle.

(4) Office of Business Mentorship.—The Commission shall establish within the Bureau an office to be known as the "Office of Business Mentorship" to provide guidance and education to covered entities and service providers regarding compliance with this subtitle.

(5) Office of consumer privacy complaint intake.—The Commission shall establish within the Bureau an office to receive complaints from the public alleging violations of this subtitle or a regulation promulgated under this subtitle.

(6) Functions.—The office established under paragraph (5) shall, in coordination with any existing complaint intake mechanisms of the Commission—

(A) establish and maintain a single toll-free telephone number, a website, and a database to facilitate the centralized collection of, monitoring of, and response to complaints described in paragraph (5);

(B) coordinate with other bureaus and offices of the Commission, the Attorney General, and other Federal agencies to route complaints to those agencies, where appropriate; and

(C) make publicly available aggregate complaint information and complaint trends, in a manner that protects personally identifiable information.

(7) Confidentiality.—The Commission shall ensure that personally identifiable information contained in complaints received under paragraph (5) is protected from public disclosure.

(f) Youth privacy and marketing division.—

(1) Establishment.—There is established within the Commission a division to be known as the "Youth Privacy and Marketing Division" (in this subsection referred to as the "Division").

(2) Director.—The Division shall be headed by a Director, who shall be appointed by the Chair of the Commission.

(3) Duties.—The Division shall be responsible for assisting the Commission in addressing, as it relates to this subtitle and section 1177 of the POPULIST Act—

(A) the privacy of covered minors; and

(B) marketing directed at covered minors.

(4) Staff.—The Director of the Division shall hire adequate staff to carry out the duties described in paragraph (3), including by hiring individuals who are experts in data protection, digital advertising, data analytics, and youth development.

(5) Reports.—Not later than 2 years after the date of enactment of this subtitle, and annually thereafter, the Commission shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives a report that includes—

(A) a description of the work of the Division regarding emerging concerns relating to youth privacy and marketing practices; and

(B) an assessment of how effectively the Division has, during the period for which the report is submitted, assisted the Commission to address youth privacy and marketing practices.

(6) Publication.—Not later than 10 days after the date on which a report is submitted under paragraph (5), the Commission shall publish the report on its website.

SEC. 566. ADDITIONAL DATA PROTECTIONS FOR COVERED MINORS.

(a) Safeguards for covered minors.—

(1) Safeguards.—A covered entity that provides an online product or service and has knowledge that an individual using or visiting such product or service is a covered minor shall provide such individual with readily accessible and easy-to-use safeguards to, as applicable—

(A) limit the ability of other users or visitors to communicate with the covered minor; and

(B) limit by default design features that result in compulsive usage of the online product or service by the covered minor.

(2) Option to limit time spent.—A covered entity described in paragraph (1) shall provide a covered minor with a readily accessible and easy-to-use option to limit the amount of time spent by the covered minor on the online product or service.

(3) Definitions.—As used in this section, the terms "compulsive usage" and "design feature" have the meanings given such terms in [section 45g of title 15, United States Code](#), as inserted by this Act.

(b) Default settings for covered minors.—A covered entity described in subsection (c)(1) shall provide that, in the case of a covered minor, the default setting for any safeguard described in subsection (a)(1) is the option available on the online product or service that provides the most protective level of control offered by the covered entity with respect to privacy and safety for that covered minor.

(c) Parental tools.—

(1) In general.—A covered entity that provides an online product or service and has knowledge that an individual using such product or service is a covered minor shall provide

readily accessible and easy-to-use parental tools for a parent to support the covered minor with respect to the use of the online product or service by that covered minor.

(2) Requirements.—The parental tools required under paragraph (1) shall include—

(A) the ability to manage the privacy and account settings of a covered minor, including any safeguard and option established under subsection (a), in a manner that allows a parent to—

(i) view the privacy and account settings; and

(ii) in the case of a child, change and control the privacy and account settings;

(B) the ability to restrict purchases and financial transactions by the covered minor, if applicable; and

(C) the ability to view metrics of total time spent on the online product or service by the covered minor and to restrict such time spent.

(3) Notice to covered minors.—A covered entity shall provide clear and conspicuous notice to a covered minor when the parental tools described in this subsection are in effect and what settings or controls have been applied.

(4) Default tools for children.—In the case of a child, a covered entity shall enable the parental tools required under paragraph (1) by default.

(d) Reporting mechanism.—

(1) Reporting tools.—A covered entity that provides an online product or service and has knowledge that 1 or more individuals using or visiting such product or service are covered minors shall provide—

(A) a readily accessible and easy-to-use means for an individual to submit a report to the covered entity of any harm to a covered minor related to the use of the online product or service;

(B) an electronic point of contact specific to matters involving harm to a covered minor; and

(C) confirmation of receipt of such report and, within the applicable time period described in paragraph (2), a substantive response to the individual that submitted the report.

(2) Timing.—A covered entity described in paragraph (1) shall establish an internal process to receive and substantively respond to a report submitted under paragraph (1) in a reasonable and timely manner, but in no case later than—

(A) 10 days after the date on which the report is received; and

(B) notwithstanding subparagraph (A), if the report involves an imminent threat to the safety of a covered minor, as promptly as needed to address the reported threat.

(e) Independent third-party audit.—

(1) In general.—Not later than July 1, 2027, and annually thereafter, each large data holder that provides an online product or service and has knowledge that 1 or more individuals using such product or service are covered minors shall have an independent, third-party auditor conduct an independent, third-party audit of the online product or service with respect to covered minors.

(2) Scope.—An audit required under paragraph (1) shall include—

(A) the number of covered minors known by the large data holder to use the online product or service during the year covered by the audit;

(B) the average and median amount of time spent by covered minors on the online product or service during the year covered by the audit;

(C) the number of times that the safeguards described in subsection (a) were exercised during the year covered by the audit;

(D) the number of times that the parental tools described in subsection (c) were exercised during the year covered by the audit;

(E) the number of reports received through the reporting mechanism described in subsection (d) during the year covered by the audit, and a description of how the large data holder handled such reports, including the rate of response and the timeliness and substantiveness of such responses;

(F) a description of whether, how, and for what purpose the large data holder collects or processes categories of covered data of covered minors; and

(G) if the large data holder has a process used to create, implement, or evaluate a design feature of the online product or service used by covered minors, a description of such process.

(3) Cooperation.—A large data holder subject to paragraph (1) shall facilitate an audit required under such paragraph by—

(A) providing or otherwise making available to the independent, third-party auditor all information and materials in the possession, custody, or control of the large data holder relevant to the audit;

(B) providing or otherwise making available to the auditor access to all networks, systems, and assets relevant to the audit; and

(C) disclosing all material facts to the auditor and not misrepresenting any material fact.

(4) Submission to Commission.—Not later than 30 days after the date on which an audit required under paragraph (1) is completed, the relevant large data holder shall submit to the Commission the results of the audit.

(f) Children and Teens Online Privacy Protection Act modernization.—

(1) Definitions.—Section 1302 of the Children's Online Privacy Protection Act of 1998 ([15 U.S.C. 6501](#)) is amended—

(A) in paragraph (2) to read as follows:

"(2) Operator.—

"(A) In general.—The term 'operator' means any person—

"(i) who, for commercial purposes, in interstate or foreign commerce operates or provides a website on the internet, an online service, an online application, or a mobile application; and

"(ii) who—

"(I) collects or maintains, either directly or through a service provider, personal information from or about the users of that website, service, or application;

"(II) allows another person to collect personal information directly from users of that website, service, or application, in which case the operator is deemed to have collected the information; or

"(III) allows users of that website, service, or application to publicly disclose personal information, in which case the operator is deemed to have collected the information.

"(B) Exclusion.—The term 'operator' does not include any nonprofit entity that would otherwise be exempt from coverage under section 5 of the Federal Trade Commission Act ([15 U.S.C. 45](#)).";

(B) in paragraph (4)—

(i) by amending subparagraph (A) to read as follows:

"(A) the release of personal information collected from a child or teen by an operator for any purpose, except where the personal information is provided to a person other than an operator who—

"(i) provides support for the internal operations of the website, online service, online application, or mobile application of the operator, excluding any activity relating to individual-specific advertising to children or teens; and

"(ii) does not disclose or use that personal information for any other purpose; and";
and

(ii) in subparagraph (B)—

(I) by inserting "or teen" after "child" each place the term appears;

(II) by striking "website or online service" and inserting "website, online service, online application, or mobile application"; and

(III) by striking "actual knowledge" and inserting "actual knowledge or knowledge fairly implied on the basis of objective circumstances";

(C) by striking paragraph (8) and inserting the following:

"(8) Personal information.—

"(A) In general.—The term 'personal information' means individually identifiable information about an individual collected online, including—

"(i) a first and last name;

"(ii) a home or other physical address including street name and name of a city or town;

"(iii) an email address;

"(iv) a telephone number;

"(v) a Social Security number;

"(vi) any other identifier that the Commission determines permits the physical or online contacting of a specific individual;

"(vii) a persistent identifier that can be used to recognize a specific child or teen over time and across different websites, online services, online applications, or mobile applications, including a customer number held in a cookie, an Internet Protocol address, a processor or device serial number, or unique device identifier, but excluding an identifier that is used by an operator solely for providing support for the internal operations of the website, online service, online application, or mobile application;

"(viii) a photograph, video, or audio file where such file contains a specific child's or teen's image or voice;

"(ix) geolocation information;

"(x) information generated from the measurement or technological processing of an individual's biological, physical, or physiological characteristics that is used to identify an individual, including—

"(I) fingerprints;

"(II) voice prints;

"(III) iris or retina imagery scans;

"(IV) facial templates;

"(V) deoxyribonucleic acid information; or

"(VI) gait; or

"(xi) information linked or reasonably linkable to a child or teen or the parents of that child or teen, including any unique identifier, that an operator collects online from the child or teen and combines with an identifier described in this subparagraph.

"(B) Exclusion.—The term 'personal information' shall not include an audio file that contains a child's or teen's voice so long as the operator—

"(i) does not request information via voice that would otherwise be considered personal information under this paragraph;

"(ii) provides clear notice of its collection and use of the audio file and its deletion policy in its privacy policy;

"(iii) only uses the voice within the audio file solely as a replacement for written words, to perform a task, or to engage with a website, online service, online application, or mobile application, including to perform a search or fulfill a verbal instruction or request; and

"(iv) only maintains the audio file long enough to complete the stated purpose and then immediately deletes the audio file and does not make any other use of the audio file prior to deletion.

"(C) Support for the internal operations of a website, online service, online application, or mobile application.—

"(i) In general.—For purposes of subparagraph (A)(vii), the term 'support for the internal operations of a website, online service, online application, or mobile application' means those activities necessary to—

"(I) maintain or analyze the functioning of the website, online service, online application, or mobile application;

"(II) perform network communications;

"(III) authenticate users of, or personalize the content on, the website, online service, online application, or mobile application;

"(IV) serve contextual advertising, provided that any persistent identifier is only used as necessary for technical purposes to serve the contextual advertisement or cap the frequency of advertising;

"(V) protect the security or integrity of the user, website, online service, online application, or mobile application;

"(VI) ensure legal or regulatory compliance; or

"(VII) fulfill a request of a child or teen as permitted by subparagraphs (A) through (C) of section 1303(b)(2).

"(ii) Condition.—Except as specifically permitted under clause (i), information collected for the activities listed in clause (i) may not be used or disclosed to contact a specific individual, including through individual-specific advertising to children or teens,

to amass a profile on a specific individual, in connection with processes that encourage or prompt use of a website, online service, online application, or mobile application, or for any other purpose.";

(D) in paragraph (9) to read as follows:

"(9) Verifiable consent.—The term 'verifiable consent' means any reasonable effort, taking into consideration available technology, including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that, in the case of a child, a parent of the child, or, in the case of a teen, the teen—

"(A) receives direct notice of the personal information collection, use, and disclosure practices of the operator; and

"(B) before the personal information of the child or teen is collected, freely and unambiguously authorizes—

"(i) the collection, use, and disclosure, as applicable, of that personal information; and

"(ii) any subsequent use of that personal information.";

(E) in paragraph (10)—

(i) in the paragraph heading, by striking "Website or online service directed to children" and inserting "Website, online service, online application, or mobile application directed to children";

(ii) by striking "website or online service" each place it appears and inserting "website, online service, online application, or mobile application"; and

(iii) by adding at the end the following:

"(C) Rule of construction.—In considering whether a website, online service, online application, or mobile application, or portion thereof, is directed to children, the Commission shall apply a totality of circumstances test and shall also consider competent and reliable empirical evidence regarding audience composition and evidence regarding the intended audience of the website, online service, online application, or mobile application."; and

(F) by adding at the end the following:

"(13) Connected device.—The term 'connected device' means a device that is capable of connecting to the internet, directly or indirectly, or to another connected device.

"(14) Online application.—The term 'online application'—

"(A) means an internet-connected software program; and

"(B) includes a service or application offered via a connected device.

"(15) Mobile application.—The term 'mobile application'—

"(A) means a software program that runs on the operating system of—

"(i) a cellular telephone;

"(ii) a tablet computer; or

"(iii) a similar portable computing device that transmits data over a wireless connection; and

"(B) includes a service or application offered via a connected device.

"(16) Geolocation information.—The term 'geolocation information' means information sufficient to identify a street name and name of a city or town.

"(17) Teen.—The term 'teen' means an individual who has attained age 13 and is under the age of 17.

"(18) Individual-specific advertising to children or teens.—

"(A) In general.—The term 'individual-specific advertising to children or teens' means advertising or any other effort to market a product or service that is directed to a specific child or teen or a connected device that is linked or reasonably linkable to a child or teen based on—

"(i) the personal information from—

"(I) the child or teen; or

"(II) a group of children or teens who are similar in sex, age, household income level, race, or ethnicity to the specific child or teen to whom the product or service is marketed;

"(ii) profiling of a child or teen or group of children or teens; or

"(iii) a unique identifier of the connected device.

"(B) Exclusions.—The term 'individual-specific advertising to children or teens' shall not include—

"(i) advertising or marketing to an individual or the device of an individual in response to the individual's specific request for information or feedback, including a child's or teen's current search query;

"(ii) contextual advertising, including when an advertisement is displayed based on the content of the website, online service, online application, mobile application, or connected device in which the advertisement appears and does not vary based on personal information related to the viewer; or

"(iii) processing personal information solely for measuring or reporting advertising or content performance, reach, or frequency, including independent measurement.

"(C) Rule of construction.—Nothing in subparagraph (A) shall be construed to prohibit an operator with actual knowledge or knowledge fairly implied on the basis of objective circumstances that a user is under the age of 17 from delivering advertising or marketing

that is age-appropriate and intended for a child or teen audience, so long as the operator does not use any personal information other than whether the user is under the age of 17."

(2) Online collection, use, disclosure, and deletion of personal information of children and teens.—Section 1303 of the Children's Online Privacy Protection Act of 1998 ([15 U.S.C. 6502](#)) is amended—

(A) by striking the heading and inserting the following: "Online collection, use, disclosure, and deletion of personal information of children and teens.";

(B) in subsection (a)—

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

"(1) In general.—It is unlawful for an operator of a website, online service, online application, or mobile application directed to children or for any operator of a website, online service, online application, or mobile application with actual knowledge or knowledge fairly implied on the basis of objective circumstances that a user is a child or teen—

"(A) to collect personal information from a child or teen in a manner that violates the regulations prescribed under subsection (b);

"(B) except as provided in subparagraphs (B) and (C) of section 1302(18), to collect, use, disclose to third parties, or maintain personal information of a child or teen for purposes of individual-specific advertising to children or teens, or to allow another person to collect, use, disclose, or maintain such information for such purpose;

"(C) to collect the personal information of a child or teen except when the collection of the personal information is—

"(i) consistent with the context of a particular transaction or service or the relationship of the child or teen with the operator, including collection necessary to fulfill a transaction or provide a product or service requested by the child or teen; or

"(ii) required or specifically authorized by Federal or State law;

"(D) to store or transfer the personal information of a child or teen outside of the United States unless the operator provides direct notice to the parent of the child, in the case of a child, or to the teen, in the case of a teen, that the child's or teen's personal information is being stored or transferred outside of the United States; or

"(E) to retain the personal information of a child or teen for longer than is reasonably necessary to fulfill a transaction or provide a service requested by the child or teen, except as required or specifically authorized by Federal or State law."; and

(ii) in paragraph (2)—

(I) in the heading, by striking "parent" and inserting "parent or teen";

(II) by striking "Notwithstanding paragraph (1)" and inserting "Notwithstanding paragraph (1)(A)";

(III) by striking "of such a website or online service"; and

(IV) by striking "subsection (b)(1)(B)(iii) to the parent of a child" and inserting "subsection (b)(1)(B)(iv) to the parent of a child or under subsection (b)(1)(C)(iv) to a teen";

(C) in subsection (b)—

(i) in paragraph (1)—

(I) in subparagraph (A)—

(aa) by striking "operator of any website" and all that follows through "from a child" and inserting "operator of a website, online service, online application, or mobile application directed to children or that has actual knowledge or knowledge fairly implied on the basis of objective circumstances that a user is a child or teen";

(bb) in clause (i), by striking "notice on the website" and inserting "clear and conspicuous notice on the website";

(cc) in clause (i), by inserting "or teens" after "children";

(dd) in clause (i), by striking ", and the operator's" and inserting ", the operator's";

(ee) in clause (i), by striking "; and" and inserting ", the rights and opportunities available to the parent of the child or teen under subparagraphs (B) and (C), and the procedures or mechanisms the operator uses to ensure that personal information is not collected from children or teens except in accordance with the regulations promulgated under this paragraph;";

(ff) in clause (ii), by striking "parental";

(gg) in clause (ii), by inserting "or teens" after "children";

(hh) in clause (ii), by striking the semicolon at the end and inserting "; and"; and

(ii) by inserting after clause (ii) the following:

"(iii) to obtain verifiable consent from a parent of a child or from a teen before using or disclosing personal information of the child or teen for any purpose that is a material change from the original purposes and disclosure practices specified to the parent of the child or the teen under clause (i);";

(II) in subparagraph (B)—

(aa) in the matter preceding clause (i), by striking "website or online service" and inserting "operator";

(bb) in clause (i), by inserting "and the method by which the operator obtained the personal information, and the purposes for which the operator collects, uses, discloses, and retains the personal information" before the semicolon;

(cc) in clause (ii), by inserting "to delete personal information collected from the child or content or information submitted by the child to a website, online service, online application, or mobile application and" after "the opportunity at any time";

(dd) in clause (ii), by striking "; and" and inserting a semicolon;

(ee) by redesignating clause (iii) as clause (iv);

(ff) by inserting after clause (ii) the following:

"(iii) the opportunity to challenge the accuracy of the personal information and, if the parent of the child establishes the inaccuracy of the personal information, to have the inaccurate personal information corrected;"; and

(gg) in clause (iv), as so redesignated, by inserting ", if such information is available to the operator at the time the parent makes the request" before the semicolon;

(III) by redesignating subparagraphs (C) and (D) as subparagraphs (D) and (E), respectively;

(IV) by inserting after subparagraph (B) the following:

"(C) require the operator to provide, upon the request of a teen under this subparagraph who has provided personal information to the operator, upon proper identification of that teen—

"(i) a description of the specific types of personal information collected from the teen by the operator, the method by which the operator obtained the personal information, and the purposes for which the operator collects, uses, discloses, and retains the personal information;

"(ii) the opportunity at any time to delete personal information collected from the teen or content or information submitted by the teen to a website, online service, online application, or mobile application and to refuse to permit the operator's further use or maintenance in retrievable form, or online collection, of personal information from the teen;

"(iii) the opportunity to challenge the accuracy of the personal information and, if the teen establishes the inaccuracy of the personal information, to have the inaccurate personal information corrected; and

"(iv) a means that is reasonable under the circumstances for the teen to obtain any personal information collected from the teen, if such information is available to the operator at the time the teen makes the request;";

(V) in subparagraph (D), as so redesignated—

(aa) by striking "a child's" and inserting "a child's or teen's"; and

(bb) by inserting "or teen" after "the child"; and

(VI) in subparagraph (E), as so redesignated, to read as follows:

"(E) require the operator to establish, implement, and maintain reasonable security practices to protect the confidentiality, integrity, and accessibility of personal information of children or teens collected by the operator, and to protect such personal information against unauthorized access.";

(ii) in paragraph (2)—

(I) in the matter preceding subparagraph (A), by striking "verifiable parental consent" and inserting "verifiable consent";

(II) in subparagraph (A)—

(aa) by inserting "or teen" after "collected from a child";

(bb) by inserting "or teen" after "request from the child"; and

(cc) by inserting "or teen or to contact another child or teen" after "to recontact the child";

(III) in subparagraph (B)—

(aa) by striking "parent or child" and inserting "parent or teen"; and

(bb) by striking "parental consent" each place it appears and inserting "verifiable consent";

(IV) in subparagraph (C)—

(aa) in the matter preceding clause (i), by inserting "or teen" after "child" each place it appears;

(bb) in clause (i), by inserting "or teen" after "child" each place it appears;

(cc) in clause (i), by inserting "or teen, as applicable," after "parent" each place it appears;

(dd) in clause (ii), by striking "without notice to the parent" and inserting "without notice to the parent or teen, as applicable,"; and

(ee) in clause (ii), by inserting "or teen" after "child" each place it appears; and

(V) in subparagraph (D)—

(aa) in the matter preceding clause (i), by inserting "or teen" after "child" each place it appears;

(bb) in clause (ii), by inserting "or teen" after "child";

(cc) in the flush text following clause (iii), by inserting "or teen, as applicable," after "parent" each place it appears; and

(dd) in the flush text following clause (iii), by inserting "or teen" after "child";

(iii) by redesignating paragraph (3) as paragraph (4);

(iv) by inserting after paragraph (2) the following:

"(3) Application to operators acting under agreements with educational agencies or institutions.—The regulations may provide that verifiable consent under paragraph (1)(A)(ii) is not required for an operator that is acting under a written agreement with an educational agency or institution, as defined in section 444 of the General Education Provisions Act, commonly known as the Family Educational Rights and Privacy Act of 1974, if the written agreement, at a minimum, requires the—

"(A) operator to—

"(i) limit its collection, use, and disclosure of the personal information from a child or teen to solely educational purposes and for no other commercial purposes;

"(ii) provide the educational agency or institution with a notice of the specific types of personal information the operator will collect from the child or teen, the method by which the operator will obtain the personal information, and the purposes for which the operator will collect, use, disclose, and retain the personal information;

"(iii) provide the educational agency or institution with a link to the operator's online notice of information practices as required under subsection (b)(1)(A)(i); and

"(iv) provide the educational agency or institution, upon request, with a means to review the personal information collected from a child or teen, to prevent further use or maintenance or future collection of personal information from a child or teen, and to delete personal information collected from a child or teen or content or information submitted by a child or teen to the operator's website, online service, online application, or mobile application;

"(B) representative of the educational agency or institution to acknowledge and agree that they have authority to authorize the collection, use, and disclosure of personal information from children or teens on behalf of the educational agency or institution, along with such authorization, their name, and title at the educational agency or institution; and

"(C) educational agency or institution to—

"(i) provide on its website a notice that identifies the operator with which it has entered into a written agreement under this subsection and provides a link to the operator's online notice of information practices as required under paragraph (1)(A)(i);

"(ii) provide the operator's notice regarding its information practices, as required under subparagraph (A)(ii), upon request, to a parent, in the case of a child, or a parent or teen, in the case of a teen; and

"(iii) upon the request of a parent, in the case of a child, or a parent or teen, in the case of a teen, request that the operator provide a means to review the personal information from the child or teen and provide the parent, in the case of a child, or parent or teen, in the case of the teen, a means to review the personal information.";

(v) by amending paragraph (4), as so redesignated, to read as follows:

"(4) Termination of service.—The regulations shall permit the operator of a website, online service, online application, or mobile application to terminate service provided to a child whose parent has refused, or a teen who has refused, under the regulations prescribed under paragraphs (1)(B)(ii) and (1)(C)(ii), to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child or teen."; and

(vi) by adding at the end the following:

"(5) Continuation of service.—The regulations shall prohibit an operator from discontinuing service provided to a child or teen on the basis of a request by the parent of the child or by the teen, under the regulations prescribed under subparagraph (B) or (C) of paragraph (1), respectively, to delete personal information collected from the child or teen, to the extent that the operator is capable of providing such service without such information.

"(6) Rule of construction.—A request made pursuant to subparagraph (B) or (C) of paragraph (1) to delete or correct personal information of a child or teen shall not be construed—

"(A) to limit the authority of a law enforcement agency to obtain any content or information from an operator pursuant to a lawfully executed warrant or an order of a court of competent jurisdiction;

"(B) to require an operator or third party to delete or correct information that—

"(i) any other provision of Federal or State law requires the operator or third party to maintain; or

"(ii) was submitted to the website, online service, online application, or mobile application of the operator by any person other than the user who is attempting to erase or otherwise eliminate the content or information, including content or information submitted by the user that was republished or resubmitted by another person; or

"(C) to prohibit an operator from—

"(i) retaining a record of the deletion request and the minimum information necessary for the purposes of ensuring compliance with a request made pursuant to subparagraph (B) or (C);

"(ii) preventing, detecting, protecting against, or responding to security incidents, identity theft, or fraud, or reporting those responsible for such actions;

"(iii) protecting the integrity or security of a website, online service, online application, or mobile application; or

"(iv) ensuring that the child's or teen's information remains deleted.

"(7) Common verifiable consent mechanism.—

"(A) In general.—

"(i) Feasibility of mechanism.—The Commission shall assess the feasibility, with notice and public comment, of allowing operators the option to use a common verifiable consent mechanism that fully meets the requirements of this title.

"(ii) Requirements.—The feasibility assessment described in clause (i) shall consider whether a single operator could use a common verifiable consent mechanism to obtain verifiable consent, as required under this title, from a parent of a child or from a teen on behalf of multiple, listed operators that provide a joint or related service.

"(B) Report.—Not later than 1 year after the date of enactment of this paragraph, the Commission shall submit to Congress a report with the findings of the assessment required by subparagraph (A).

"(C) Regulations.—If the Commission finds that the use of a common verifiable consent mechanism is feasible and would meet the requirements of this title, the Commission shall issue regulations to permit the use of a common verifiable consent mechanism in accordance with the findings outlined in such report.";

(D) in subsection (c), by striking "a regulation prescribed under subsection (a)" and inserting "subparagraph (B), (C), (D), or (E) of subsection (a)(1), or of a regulation prescribed under subsection (b),"; and

(E) by striking subsection (d) and inserting the following:

"(d) Relationship to State law.—The provisions of this title shall preempt any State law, rule, or regulation only to the extent that such State law, rule, or regulation conflicts with a provision of this title. Nothing in this title shall be construed to prohibit any State from enacting a law, rule, or regulation that provides greater protection to children or teens than the provisions of this title."

(3) Safe harbors.—Section 1304 of the Children's Online Privacy Protection Act of 1998 ([15 U.S.C. 6503](#)) is amended—

(A) in subsection (b)(1), by inserting "and teens" after "children"; and

(B) by adding at the end the following:

"(d) Publication.—

"(1) In general.—Subject to the restrictions described in paragraph (2), the Commission shall publish on the internet website of the Commission any report or documentation required by regulation to be submitted to the Commission to carry out this section.

"(2) Restrictions on publication.—The restrictions described in section 6(f) and section 21 of the Federal Trade Commission Act ([15 U.S.C. 46\(f\)](#), [57b–2](#)) applicable to the disclosure of information obtained by the Commission shall apply in the same manner to the disclosure under this subsection of information obtained by the Commission from a report or documentation described in paragraph (1).".

(4) Actions by States.—Section 1305 of the Children's Online Privacy Protection Act of 1998 ([15 U.S.C. 6504](#)) is amended—

(A) in subsection (a)(1)—

(i) in the matter preceding subparagraph (A), by inserting "section 1303(a)(1) or" before "any regulation"; and

(ii) in subparagraph (B), by inserting "section 1303(a)(1) or" before "the regulation"; and

(B) in subsection (d)—

(i) by inserting "section 1303(a)(1) or" before "any regulation"; and

(ii) by inserting "section 1303(a)(1) or" before "that regulation".

(5) Administration and applicability.—Section 1306 of the Children's Online Privacy Protection Act of 1998 ([15 U.S.C. 6505](#)) is amended—

(A) in subsection (b)—

(i) in paragraph (1), by striking ", in the case of" and all that follows through "the Board of Directors of the Federal Deposit Insurance Corporation;" and inserting "by the appropriate Federal banking agency, with respect to any insured depository institution, as those terms are defined in section 3 of the Federal Deposit Insurance Act ([12 U.S.C. 1813](#));"; and

(ii) by striking paragraph (2) and redesignating paragraphs (3) through (6) as paragraphs (2) through (5), respectively;

(B) in subsection (d)—

(i) by inserting "section 1303(a)(1) or" before "a rule"; and

(ii) by striking "such rule" and inserting "section 1303(a)(1) or a rule of the Commission under section 1303"; and

(C) by adding at the end the following:

"(f) Determination of whether an operator has knowledge fairly implied on the basis of objective circumstances.—

"(1) Rule of construction.—For purposes of enforcing this title or a regulation promulgated under this title, in making a determination as to whether an operator has knowledge fairly implied on the basis of objective circumstances that a specific user is a child or teen, the

Commission or State attorneys general shall rely on competent and reliable evidence, taking into account the totality of the circumstances, including whether a reasonable and prudent person under the circumstances would have known that the user is a child or teen.

"(2) Commission guidance.—

"(A) In general.—Not later than 180 days after the date of enactment of this subsection, the Commission shall issue guidance to provide information, including best practices and examples for operators to understand the Commission's determination of whether an operator has knowledge fairly implied on the basis of objective circumstances that a user is a child or teen.

"(B) Limitation.—No guidance issued by the Commission with respect to this title shall confer any rights on any person, State, or locality, or operate to bind the Commission or any person to the approach recommended in such guidance. In any enforcement action brought pursuant to this title, the Commission or State attorney general, as applicable, shall allege a specific violation of a provision of this title. The Commission or State attorney general, as applicable, may not base an enforcement action on, or execute a consent order based on, practices that are alleged to be inconsistent with any such guidance, unless the practices allegedly violate this title. For purposes of enforcing this title or a regulation promulgated under this title, State attorneys general shall take into account any guidance issued by the Commission under subparagraph (A).

"(g) Additional requirement.—Any regulations issued under this title shall include a description and analysis of the impact of proposed and final rules on small entities under chapter 6 of [title 5, United States Code](#)."

(6) Reports and studies.—

(A) Oversight report.—Not later than 3 years after the date of enactment of this subsection, the Commission shall submit to Congress a report on the processes of platforms that offer mobile and online applications for ensuring that those applications that are websites, online services, online applications, or mobile applications directed to children operate in accordance with—

(i) the Children's Online Privacy Protection Act of 1998, as amended by this subsection, and rules promulgated under such Act; and

(ii) rules promulgated by the Commission under section 18 of the Federal Trade Commission Act ([15 U.S.C. 57a](#)) relating to unfair, deceptive, or abusive acts or practices in marketing.

(B) Enforcement report.—Not later than 1 year after the date of enactment of this subsection, and each year thereafter, the Commission shall submit to Congress a report that addresses, at a minimum—

(i) the number of actions brought by the Commission during the reporting year to enforce the Children's Online Privacy Protection Act of 1998 and the outcome of each such action;

(ii) the total number of investigations or inquiries into potential violations of such Act during the reporting year;

(iii) the total number of open investigations or inquiries into potential violations of such Act as of the time the report is submitted;

(iv) the number and nature of complaints received by the Commission relating to an allegation of a violation of such Act during the reporting year; and

(v) policy or legislative recommendations to strengthen online protections for children and teens.

(C) Teen financial technology privacy study.—The Comptroller General of the United States shall conduct a study on the privacy of teens who use financial technology products, including a study to—

(i) identify the types of financial technology products that teens are using;

(ii) identify the potential risks to teens' privacy from using such financial technology products; and

(iii) determine whether existing laws are sufficient to address such risks to teens' privacy.

(D) Report.—Not later than 1 year after the date of enactment of this subsection, the Comptroller General shall submit to Congress a report containing the results of the study conducted under subparagraph (C), together with recommendations for such legislation and administrative action as the Comptroller General determines appropriate.

(g) Report by the Inspector General.—

(1) In general.—Not later than 2 years after the date of enactment of this subtitle, and biennially thereafter, the Inspector General of the Commission shall submit to the Commission and to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives a report regarding the safe harbor provisions in section 1304 of the Children's Online Privacy Protection Act of 1998 ([15 U.S.C. 6503](#)), which shall include—

(A) an analysis of whether the safe harbor provisions are—

(i) operating fairly and effectively; and

(ii) effectively protecting the interests of covered minors; and

(B) any proposal or recommendation for policy changes that would improve the effectiveness of the safe harbor provisions.

(2) Publication.—Not later than 10 days after the date on which a report is submitted under paragraph (1), the Commission shall publish the report on the website of the Commission.

(h) Rule of construction.—Nothing in this section shall be construed to prevent a covered entity from taking reasonable measures to protect the privacy, safety, or security of covered minors consistent with this subtitle and other applicable law.

SEC. 567. BANNING SURVEILLANCE ADVERTISING.

(a) Definitions.—In this section—

(1) Advertisement.—The term "advertisement" means information provided by an advertiser to an advertising facilitator that the advertising facilitator, in exchange for monetary consideration or another thing of value, disseminates to an individual, connected device, or group of individuals or connected devices.

(2) Advertiser.—

(A) In general.—The term "advertiser" means a person to the extent such person, directly or indirectly, provides an advertising facilitator with monetary consideration or another thing of value for the dissemination of an advertisement to an individual, connected device, or group of individuals or connected devices.

(B) Exclusion.—The term "advertiser" does not include a natural person, except to the extent such person is engaged in a commercial activity that is more than de minimis.

(3) Advertising facilitator.—

(A) In general.—The term "advertising facilitator" means a person to the extent such person—

(i) receives monetary consideration or another thing of value to disseminate an advertisement to an individual, connected device, or group of individuals or connected devices; and

(ii) obtains or processes personal information with respect to the dissemination of the advertisement.

(B) Exclusion.—The term "advertising facilitator" does not include a natural person, except to the extent such person is engaged in a commercial activity that is more than de minimis.

(4) Connected device.—The term "connected device" means any electronic equipment that is—

(A) primarily designed for or marketed to consumers;

(B) capable of connecting to the internet or another communication network; and

(C) capable of sending, receiving, or processing personal information.

(5) Contents.—The term "contents", when used with respect to any communication, has the meaning given such term in [section 2510 of title 18](#), United States Code.

(6) Disseminate.—The term "disseminate" means, with respect to an advertisement, to transmit, display, or otherwise disseminate the advertisement electronically or through communication by wire or radio.

(7) Dissemination.—The term "dissemination" means, with respect to an advertisement, the transmission, display, or other dissemination of the advertisement electronically or through communication by wire or radio.

(8) Indian lands.—The term "Indian lands" includes—

(A) any Indian country of an Indian Tribe (as such term is defined in [section 1151 of title 18](#), United States Code);

(B) any land in Alaska owned, pursuant to the Alaska Native Claims Settlement Act ([43 U.S.C. 1601 et seq.](#)), by an Indian Tribe that is a Native village or by a Village Corporation (as such terms are defined in section 3 of that Act ([43 U.S.C. 1602](#))) that is associated with an Indian Tribe; and

(C) any land that is part or all of a Tribal designated statistical area associated with an Indian Tribe, or is part or all of an Alaska Native village statistical area associated with an Indian Tribe, as defined by the Bureau of the Census for the purposes of the most recent decennial census.

(9) Indian Tribe.—The term "Indian Tribe" has the meaning given such term in section 4 of the Indian Self-Determination and Education Assistance Act ([25 U.S.C. 5304](#)).

(10) Obtain.—The term "obtain" means, with respect to personal information, to obtain such information in any manner, except when solely transmitting, routing, providing intermediate storage for, or providing connections for such information through a system or network.

(11) Personal information.—The term "personal information" means data linked or reasonably linkable to an individual or connected device, including—

(A) data inferred or derived about the individual or connected device from other obtained data, if such data is still linked or reasonably linkable to the individual or connected device;

(B) contents of communications;

(C) internet browsing history and online activity; and

(D) a unique identifier used for the purposes of targeting the dissemination of an advertisement.

(12) Recognized place.—

(A) In general.—The term "recognized place" means any of the following:

(i) A State.

(ii) Indian lands.

(iii) A county, municipality, city, town, township, village, borough, or similar unit of general government that is incorporated pursuant to a State law.

(iv) A census designated place (as defined in the most recent glossary of the Bureau of the Census).

(v) A designated market area (as defined in [section 122\(j\) of title 17](#), United States Code).

(vi) A congressional district.

(vii) Any possession of the United States.

(B) Exclusions.—The term "recognized place" does not include—

(i) a subdivision of any item listed in subparagraph (A) that is not itself listed in such subparagraph; or

(ii) a ZIP Code.

(13) Target.—

(A) In general.—The term "target" means, with respect to the dissemination of an advertisement, to perform or cause to be performed any computational process designed to select an individual, connected device, or group of individuals or connected devices to which to disseminate the advertisement based on personal information pertaining to the individual or connected device or to the individuals or connected devices that make up the group.

(B) Exclusions.—The term "target" does not include, with respect to the dissemination of an advertisement, the performance or causing the performance of any computational process undertaken solely for transmitting, routing, providing intermediate storage for, or providing connections for the advertisement through a system or network.

(14) Third party.—The term "third party" includes, with respect to an advertiser or an advertising facilitator, a subsidiary, a corporate affiliate, or other related party of the advertiser or advertising facilitator.

(b) Prohibition on targeted advertising.—

(1) In general.—An advertiser or an advertising facilitator may not—

(A) target the dissemination of an advertisement; or

(B) knowingly enable an advertiser (in the case of an advertising facilitator), advertising facilitator (in the case of an advertiser), or third party to target the dissemination of an advertisement, including by providing a list of individuals or connected devices, contact information of an individual, or a unique identifier or other personal information that can be used to identify an individual or a connected device.

(2) Contextual advertisements.—

(A) In general.—For purposes of paragraph (1), an advertising facilitator shall not be considered to target the dissemination of an advertisement if the advertisement—

(i) is disseminated based on information the individual is viewing, engaging with, or searched for; and

(ii) is displayed in close proximity to such information.

(B) Prohibition on further use.—Information obtained in connection with subparagraph (A) may not be used to target additional advertisements or to knowingly enable an advertiser or third party to target the dissemination of additional advertisements.

(3) Exemptions for recognized places.—The prohibition in this subsection shall not apply to the dissemination of an advertisement targeted exclusively on a recognized place.

(c) Effective date.—This section shall be effective 90 days after the date of enactment of this Act.

SEC. 568. DATA PORTABILITY AND INTEROPERABILITY.

(a) Definitions.—In this section:

(1) Affirmative disclosure consent.—The term "affirmative disclosure consent" means an affirmative action of the consumer to make a choice following a clear and conspicuous disclosure to the consumer, separate and apart from any "privacy policy", "terms of service", "consent for research", or other similar document, of—

(A) the types of personal information that the covered platform will disclose to third parties;

(B) the reason for such disclosures;

(C) the identity of all such third parties;

(D) any opportunities consumers have to decline or rescind consent for such disclosures; and

(E) how consumers may exercise any such opportunities.

An affirmative action does not include obtaining a consumer's approval for a preselected default option.

(2) Business user.—The term "business user" means a person that utilizes or plans to utilize the covered platform for the sale or provision of products or services.

(3) Clear and conspicuous disclosure.—The term "clear and conspicuous disclosure" means that a required disclosure is difficult to miss such that it is easily noticeable and easily understandable by ordinary consumers, including in all of the following ways:

(A) In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television

advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure is made through only one means.

(B) A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

(C) An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

(D) In any communication using an interactive electronic medium, such as the internet or software, the disclosure must be unavoidable.

(E) The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.

(F) The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

(G) The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

(H) When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable members of that group.

(4) Commission.—The term "Commission" means the Federal Trade Commission.

(5) Competitor.—The term "competitor" means an online platform that competes with, or is a potential competitor to, a covered platform.

(6) Covered platform.—The term "covered platform" means an online platform that—

(A) during any month in either of the previous 2 calendar years—

(i) had at least 50,000,000 United States-based monthly active users on the online platform; or

(ii) had at least 100,000 United States-based monthly active business users on the platform;

(B) during either of the previous 2 calendar years, was owned or controlled by a person with net annual sales, or a market capitalization, greater than \$600,000,000,000, as adjusted and published for each fiscal year beginning after September 30, 2026, in the same manner as provided in section 8(a)(5) of the Clayton Act ([15 U.S.C. 19\(a\)\(5\)](#)), for the year then ended over the level for the year ending September 30, 2026;

(C) is a critical trading partner for the sale or provision of any product or service offered on or directly related to the online platform; or

(D) is designated as a covered platform under subsection (f).

(7) Covered platform operator.—The term "covered platform operator" means a person that, directly or indirectly, with respect to a covered platform—

(A) holds 25 percent or more of the stock;

(B) has the right to 25 percent or more of the profits;

(C) has the right to 25 percent or more of the assets in the event of the platform's dissolution;

(D) if the platform is a corporation, has the power to designate 25 percent or more of the directors;

(E) if the platform is a trust, has the power to designate 25 percent or more of the trustees; or

(F) otherwise exercises substantial control over such platform.

(8) Critical trading partner.—The term "critical trading partner" means a trading partner that has the ability to restrict or impede—

(A) the access of a business user to its users or customers; or

(B) the access of a business user to a tool or service that it needs to effectively serve its users or customers.

(9) Data.—

(A) In general.—The term "data" means information that is collected by or provided to a covered platform or a competitor that is linked, or reasonably linkable, to a specific user, user device, or customer of the covered platform or competitor, but does not include proprietary data that does not pertain to the user or a user device of such covered platform or competitor.

(B) Rulemaking.—Not later than 90 days after the date of enactment of this Act, the Commission shall adopt interim final rules in accordance with [section 553 of title 5](#), United States Code, and shall thereafter promulgate final regulations after notice and comment, to clarify the term "data" for purposes of implementing and enforcing this section; provided the Commission shall narrowly construe the term "proprietary data."

(10) Interoperability interface.—The term "interoperability interface" means an electronic interface maintained by a covered platform for purposes of achieving interoperability.

(11) Online platform.—The term "online platform" means a website, online or mobile application, operating system, digital assistant, or online service that—

(A) enables a user to generate content that can be viewed by other users on the platform or to interact with other content on the platform;

(B) facilitates the offering, sale, purchase, payment, or shipping of goods or services, including software applications, between and among consumers or businesses not controlled by the platform; or

(C) enables user searches or queries that access or display a large volume of information.

(b) Unfair method of competition.—A violation of this section, or standards issued pursuant to this section, by a person, partnership, or corporation operating a covered platform, in or affecting commerce, shall be an unfair method of competition in violation of section 5(a)(1) of the Federal Trade Commission Act ([15 U.S.C. 45\(a\)\(1\)](#)).

(c) Portability.—

(1) In general.—A covered platform shall maintain a set of transparent, third-party-accessible interfaces (including application programming interfaces) to enable the secure transfer of data to a user, or with the affirmative disclosure consent of a user, to an online platform at the direction of a user, in a structured, commonly used, and machine-readable format that complies with the standards issued pursuant to subsection (f).

(2) (A) Data security.—An online platform that receives ported user data from a covered platform shall reasonably secure any user data it acquires, and shall take reasonable steps to avoid introducing security risks to data or the covered platform's information systems.

(B) Violation.—A failure to comply with this paragraph is a violation of this section and subject to enforcement under section 569.

(C) Termination of access.—The Commission may require the covered platform to cease the transfer of data to an online platform that the Commission finds has violated this paragraph or standards adopted by the Commission under subsection (f).

(3) Portability obligations.—In order to achieve portability under paragraph (1), a covered platform shall comply with the standards issued under subsection (f) by the Commission.

(d) Interoperability.—

(1) (A) In general.—A covered platform shall maintain a set of transparent, third-party-accessible interfaces (including application programming interfaces) to facilitate and maintain interoperability with competitors through an interoperability interface, based on fair, reasonable, and nondiscriminatory terms.

(B) Presumption.—It shall be a rebuttable presumption that a covered platform is providing access on fair, reasonable, and nondiscriminatory terms if—

(i) such platform establishes and maintains interoperability through an open standard established under subsection (f); and

(ii) with respect to a covered platform that maintains interoperability between more than 1 online platform affiliated with such covered platform, offers a functionally equivalent version of that interface to competitors.

(2) (A) Data security.—A competitor that accesses an interoperability interface of a covered platform shall reasonably secure any user data it acquires, processes, or transmits, and shall take reasonable steps to avoid introducing security risks to user data or the covered platform's information systems.

(B) Violation.—A failure to comply with this paragraph is a violation of this section and subject to enforcement under section 569.

(C) Termination of access.—The Commission may require the covered platform to cease interoperating with a competitor that the Commission finds has violated this paragraph or standards adopted by the Commission under subsection (f).

(3) Interoperability obligations.—A covered platform shall, in compliance with the standards issued pursuant to subsection (f), facilitate the importation of a user's data—

(A) from such user; or

(B) with the affirmative disclosure consent of a user, from an online platform at the direction of a user.

(4) Reasonable thresholds, access standards, fees, and privacy and security protections.—

(A) In general.—A covered platform may establish reasonable thresholds related to the frequency, nature, and volume of requests by a competitor to access resources maintained by the covered platform, beyond which the covered platform may assess a reasonable fee for such access.

(B) Usage expectations.—A covered platform may establish fair, reasonable, and nondiscriminatory usage expectations to govern access by competitors, including fees or penalties for competitors that exceed those usage expectations.

(C) Limitation on fees and usage expectations.—Any fees, penalties, or usage expectations assessed under subparagraphs (A) and (B) shall be reasonably proportional to the cost, complexity, and risk to the covered platform of providing such access.

(D) Notice.—A covered platform shall provide public notice of any fees, penalties, or usage expectations established under this paragraph, including reasonable advance notice of any changes.

(E) Security and privacy standards.—A covered platform shall, consistent with industry best practices, set privacy and security standards for access by competitors to the extent reasonably necessary to address a threat to the covered platform or user data, and shall report any suspected violations of those standards to the Commission.

(5) Prohibited changes to interfaces; interface information; notice of changes.—

(A) Prohibited changes.—A change to an interoperability interface or terms of use made with the purpose, or substantial effect, of unreasonably denying access or undermining interoperability for competitors shall be considered a violation of the duty under paragraph (1) to facilitate and maintain interoperability on fair, reasonable, and nondiscriminatory terms.

(B) Interface information.—

(i) In general.—Not later than 120 days after the adoption of a rule by the Commission under subsection (f), a covered platform shall make available to competitors, which may be provided through public notice, complete and accurate documentation describing access to the interoperability interface required under this subsection.

(ii) Contents.—The documentation required under clause (i)—

(I) is limited to interface documentation necessary to achieve development and operation of interoperable products and services; and

(II) does not require the disclosure of the source code of a covered platform.

(C) Notice of changes.—A covered platform shall provide reasonable advance notice to competitors, which may be provided through public notice, of any change to an interoperability interface maintained by the covered platform that will affect the interoperability with competitors.

(6) Data minimization.—

(A) Noncommercialization by a covered platform.—A covered platform shall not collect, use, or share user data obtained from a business user through the interoperability interface except for the purposes of safeguarding the privacy and security of such information or maintaining interoperability of services.

(B) Noncommercialization of data on a covered platform.—A business user shall not collect, use, or share the data of a user on a covered platform except for the purposes of safeguarding the privacy or security of such data, maintaining interoperability of services, fulfilling a transaction requested by the user, providing customer service, shipping or delivery, processing returns or refunds, warranty support, fraud prevention reasonably necessary to complete or protect a transaction requested by the user, or another purpose specifically and separately authorized by the user.

(e) Technical committee.—

(1) Establishment.—Not later than 90 days after the date of enactment of this Act, the Commission shall establish a technical committee, whose size and membership is within the sole discretion of the Commission except as specified in paragraph (2), to assist the Commission with considerations relating to—

(A) implementation and technical aspects of the requirements under subsections (c) and (d); and

(B) technical standards described under section 589(d) of this Act.

(2) Composition.—A technical committee shall include—

(A) representatives of businesses that, in the judgment of the Commission, utilize or compete with the covered platform;

(B) representatives of competition or privacy advocacy organizations, and independent academics that possess technical, legal, economic, financial, or other knowledge that the Commission may deem useful;

(C) a representative from the National Institute of Standards and Technology; and

(D) representatives of a covered platform, which, if required by the Commission, shall provide a nonvoting advisory member to provide consultation and other aid to the technical committee. A failure by the covered platform to participate in good faith in the development of standards by the technical committee shall be a violation of this section.

(3) General responsibilities.—A technical committee established under this subsection shall meet regularly to provide information, analysis, and recommendations to the Commission on the standards of portability and interoperability, the technical standards under section 589(d) of this Act, and any changes to such standards. With respect to the requirements of subsections (c) and (d), these standards shall—

(A) seek to reduce or eliminate network effects that limit competition with the covered platform;

(B) establish data security and privacy protections for data portability and interoperability;

(C) seek to prevent fraudulent, malicious, or abusive activity by competitors; and

(D) establish reasonable thresholds related to the frequency, nature, and volume of requests by a competitor to access resources maintained by the covered platform, beyond which the covered platform may assess a reasonable fee for such access that shall be reasonably proportional to the cost, complexity, and risk to the covered platform of providing such access, and do not limit the ability or deter the incentive of a competitor to interoperate with the covered platform.

(4) Role.—The role of technical committees is advisory in nature, and such committees shall have no implementation or enforcement authority. However, the Commission shall give strong consideration to the recommendations of such committees in implementing this section.

(5) Nonapplicability of the Federal Advisory Committee Act.—The requirements of [chapter 10 of title 5](#), United States Code (commonly known as the 'Federal Advisory Committee Act'), shall not apply with respect to the technical committees.

(f) Implementation.—

(1) Official designation.—

(A) In general.—An online platform that meets the requirements under subparagraph (A), (B), or (C) of subsection (a)(6) shall be designated a covered platform by the Commission.

(B) Additional designation authority.—The Commission may officially designate as a covered platform any online platform whose designation would advance the goals of this

section, including reducing or eliminating network effects that limit competition with a covered platform, by publishing the designation in the Federal Register.

(C) Effect of designation.—After designating an online platform as a covered platform, the Commission shall issue standards of interoperability specific to the covered platform which incorporate the requirements of subsections (c) and (d).

(D) Duration of designation.—The designation of an online platform as a covered platform under subparagraph (A) or (B) shall apply indefinitely, regardless of whether there is a change in control or ownership of the platform, unless the Commission removes the designation under paragraph (3).

(2) Judicial review.—

(A) In general.—Any party that is subject to a covered platform designation pursuant to paragraph (1)(B), a final order issued in any district court, or a final order of the Commission issued in an administrative adjudicative proceeding may, within 30 days after the issuance of such order, petition for review of such order in the United States Court of Appeals for the District of Columbia Circuit.

(B) Treatment of findings.—In a proceeding for judicial review of a covered platform designation pursuant to paragraph (1) or a final order of the Commission, the findings of the Commission as to the facts, if supported by evidence, shall be conclusive.

(3) Removal of designation.—

(A) Request.—If an online platform designated as a covered platform under paragraph (1) ceases to meet the qualifications for such designation, the platform may submit to the Commission a request for removal of the designation, together with evidence that the platform no longer so qualifies.

(B) Determination.—

(i) In general.—Not later than 120 days after receiving a request under subparagraph (A), the Commission shall determine whether to grant the request and, if the Commission grants the request, remove the platform from the public list under paragraph (4).

(ii) Denied requests.—A denial under clause (i) of a request submitted under subparagraph (A) shall constitute final agency action for purposes of chapter 7 of [title 5, United States Code](#).

(4) Public list.—

(A) In general.—The Commission shall maintain and periodically update on its website a public list of designated covered platforms.

(B) Omission not dispositive.—Omission from the public list under subparagraph (A) shall not by itself establish that a person is not a covered platform.

(5) Rulemaking and technical standards.—

(A) In adopting the standards implementing the requirements of subsections (c) and (d), the Commission shall seek to encourage entry into commerce by—

(i) reducing or eliminating the network effects that limit competition with the covered platform;

(ii) ensuring that competitors interconnect with the covered platform on fair and nondiscriminatory terms; and

(iii) protecting data security and privacy.

(B) The Commission shall—

(i) establish a technical committee pursuant to subsection (e) to develop proposed standards implementing the requirements of subsections (c) and (d) as they apply to a specific covered platform;

(ii) issue such open standards in accordance with [section 553 of title 5](#), United States Code; and

(iii) reject standards that would unreasonably deny access, undermine interoperability, or be unduly disruptive to interoperability.

(C) In issuing standards under this paragraph, the Commission shall consult with the Director of the National Institute of Standards and Technology and may incorporate model technical standards published by the Director for interoperable classes of online communications or information services.

(6) Compliance assessment.—The Commission shall regularly assess compliance by covered platforms with the provisions of this section and may—

(A) undertake such investigation as appropriate to render this assessment;

(B) issue subpoenas and civil investigative demands for relevant information, including any information that is necessary to effectuate the goals of subsections (c) and (d), and consult with other agencies as appropriate; and

(C) prescribe such other rules in accordance with [section 553 of title 5](#), United States Code as may be necessary and appropriate to carry out subsections (c) and (d).

(7) Agency complaints.—The Commission shall establish procedures under which a user, covered platform, or business user may file a complaint alleging a violation of this section.

(8) Reciprocity.—

(A) Opt in to participate.—A business user or competitor shall not be required to comply with the portability or interoperability requirements of this section unless it chooses to—

(i) initiate the secure export of data under subsection (c); or

(ii) access an interoperability interface under subsection (d) to import data.

(B) Reciprocal transfer obligation.—A business user or competitor that makes an election described in subparagraph (A)—

(i) shall, upon request of a user, facilitate the secure transfer of the data of that user, in a format consistent with the standards issued under this section, to—

(I) such user; or

(II) another entity, at the direction of the user and pursuant to the user's affirmative disclosure consent;

(ii) may cease importation of data through the interoperability interface at any time, provided such online platform or competitor shall first provide—

(I) notice to the Commission in such form as they may by regulation require; and

(II) clear and conspicuous notice to affected users; and

(iii) may cease exportation of data under subsection (c) no less than 90 days after ceasing importation of data under clause (ii).

(C) No effect on covered-platform duties.—Nothing in this paragraph shall be construed to relieve a covered platform of an obligation imposed on that covered platform under subsection (c) or (d).

SEC. 569. REGULATIONS AND ENFORCEMENT.

(a) Regulations.—The Commission shall promulgate regulations in accordance with [section 553 of title 5](#), United States Code, as necessary to carry out this subtitle.

(b) Enforcement.—

(1) Federal Trade Commission.—A violation of this subtitle or a regulation promulgated under this subtitle shall be treated as a violation of a rule defining an unfair, deceptive, or abusive act or practice under section 18 of the Federal Trade Commission Act ([15 U.S.C. 57a](#)).

(A) Powers of the Commission.—Except as provided in subparagraphs (B) and (C), the Commission shall enforce this subtitle and the regulations promulgated under this subtitle in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act ([15 U.S.C. 41 et seq.](#)) were incorporated into and made a part of this subtitle, and any person who violates this subtitle or a regulation promulgated under this subtitle shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

(B) Exclusive litigation authority.—Notwithstanding section 16(a) of the Federal Trade Commission Act ([15 U.S.C. 56\(a\)](#)), the Commission shall have exclusive authority to commence or defend, and supervise the litigation of, any action for a violation of this subtitle or a regulation promulgated under this subtitle, and any appeal of such action, in its own name by any of its attorneys designated by it for such purpose, without first referring the matter to the Attorney General.

(C) Common carriers and nonprofit organizations.—Notwithstanding section 4, section 5(a)(2), or section 6 of the Federal Trade Commission Act ([15 U.S.C. 44](#); [45\(a\)\(2\)](#); [46](#)), or any jurisdictional limitation of the Commission, the Commission shall also enforce this subtitle and the regulations promulgated under this subtitle in the same manner provided in subparagraphs (A) and (B) with respect to—

(i) common carriers subject to the Communications Act of 1934 ([47 U.S.C. 151 et seq.](#)) and all Acts amendatory thereof and supplementary thereto; and

(ii) organizations not organized to carry on business for their own profit or that of their members.

(D) Savings clause.—Nothing in this subtitle shall be construed to limit the authority of the Commission under any other provision of law.

(E) Intervention by the Commission.—The Commission may intervene in any civil action brought under paragraphs (2) or (3), and upon intervening may be heard on all matters arising in the civil action, and file petitions for appeal of a decision in the civil action.

(2) States.—

(A) In general.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of the State has been or is threatened or adversely affected by an act or practice in violation of this subtitle or a regulation promulgated under this subtitle, the attorney general of the State may, as *parens patriae*, bring a civil action on behalf of the residents of the State in an appropriate district court of the United States or an appropriate State court to obtain appropriate relief.

(B) Commission intervention.—

(i) Notice to the Commission.—

(I) In general.—Except as provided in subclause (III), the attorney general of a State shall notify the Commission in writing that the attorney general intends to bring a civil action under subparagraph (A) before initiating the civil action.

(II) Contents.—The notification required by subclause (I) with respect to a civil action shall include a copy of the complaint to be filed to initiate the civil action.

(III) Exception.—If it is not feasible for the attorney general of a State to provide the notification required by subclause (I) before initiating a civil action under subparagraph (A), the attorney general shall notify the Commission immediately upon instituting the civil action.

(ii) Intervention by the Commission.—The Commission may—

(I) intervene in any civil action brought by the attorney general of a State under subparagraph (A); and

(II) upon intervening—

(aa) remove the civil action to the appropriate district court of the United States, if the action was not originally brought in such court;

(bb) be heard on all matters arising in the civil action; and

(cc) file petitions for appeal of a decision in the civil action.

(iii) Investigatory powers.—Nothing in this paragraph may be construed to prevent the attorney general of a State from exercising the powers conferred on the attorney general by the laws of the State to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

(C) Action by the Commission.—If the Commission institutes a civil action with respect to a violation of this subtitle or a regulation promulgated under this subtitle, the attorney general of a State may not, during the pendency of such action, bring a civil action under subparagraph (A) against any defendant named in the complaint of the Commission for the violation with respect to which the Commission instituted such action.

(D) Actions by other State officials.—In addition to civil actions brought by attorneys general under subparagraph (A), any other officer of a State who is authorized by the State to do so may bring a civil action under such subparagraph, subject to the same requirements and limitations that apply under this paragraph to civil actions brought by attorneys general.

(E) Penalties.—The maximum civil monetary penalty for violations subject to civil penalties under this paragraph shall be the same as the maximum civil penalty amount for violations of unfair, deceptive, or abusive trade practices under the Federal Trade Commission Act, as periodically published by the Commission pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990, as amended, and any corresponding rules ([16 C.F.R. 1.98](#)).

(F) Savings provision.—Nothing in this paragraph may be construed to prohibit an attorney general or authorized official of a State from initiating or continuing any proceeding in a court of the State for a violation of any civil or criminal law of the State.

(3) Private civil action.—

(A) In general.—Any individual alleging a violation of this subtitle or a regulation promulgated under this subtitle may bring a civil action in any Federal or State court of competent jurisdiction, provided that a plaintiff notifies the Commission in writing before filing such action, such notification including a copy of the complaint, except that if it is not feasible to provide the required notification prior to initiating a civil action under this paragraph, such notification shall be made immediately upon instituting the civil action.

(B) Relief.—In a civil action in which the plaintiff prevails, the court may award an amount equal to, in the case of a negligent violation, not less than \$100 and not greater than \$1,000 per violation, or in the case of a reckless, knowing, willful, or intentional violation, not less than \$500 and not greater than \$5,000 per violation, reasonable

attorney's fees and litigation costs, and any other relief, including equitable or declaratory relief, that the court determines appropriate.

(C) Injury in fact.—A violation of this subtitle or a regulation promulgated under this subtitle with respect to the covered data of an individual constitutes a concrete and particularized injury in fact to that individual.

(c) Rule of construction.—Nothing in this subtitle shall be construed—

(1) to preempt or limit any Federal, State, local, or Tribal law that provides equal or greater protection for privacy, data security, data portability, interoperability, or protection against deceptive, manipulative, misleading, abusive, or intrusive advertising or data practices; or

(2) to limit the authority of the Federal Trade Commission, the Attorney General, the Federal Communications Commission, the Secretary of Health and Human Services, or any other Federal agency under any other provision of law.

Subtitle E—Rein In Big Tech

SEC. 571. COMPETITION AND TRANSPARENCY IN DIGITAL ADVERTISING.

(a) Digital advertising trading transparency and competition.—The Clayton Act is amended by inserting after section 8 ([15 U.S.C. 19](#)) the following:

"Sec. 8A. Competition and transparency in digital advertising.

"(a) Definitions.—In this section:

"(1) Applicability date.—The term 'applicability date' means the date that is 1 year after the date of enactment of this section.

"(2) Brokerage customer.—The term 'brokerage customer' means a person who has purchased or sold digital advertisements, or directly related goods or services, through a buy-side brokerage or a sell-side brokerage.

"(3) Buy-side brokerage.—The term 'buy-side brokerage' means a person in the business of effecting transactions on digital advertising exchanges, including by offering software or services that assist in serving or displaying digital advertisements, for other buyers.

"(4) Digital advertisement.—The term 'digital advertisement' means an advertisement that is served electronically over a computer network, including the internet.

"(5) Digital advertising exchange.—The term 'digital advertising exchange' means a person who constitutes, maintains, or provides a marketplace for or facilitates bringing together buyers and 1 or more sellers of digital advertisements, or for otherwise performing with respect to digital advertising the functions commonly performed by a digital advertising marketplace.

"(6) Digital advertising revenue.—The term 'digital advertising revenue' means the greater of—

"(A) global revenue derived from or directly related to the operation of a digital advertising exchange, a buy-side brokerage, or a sell-side brokerage;