CONGRESS.GOV

H.R.8818 - American Privacy Rights Act of 2024

118th Congress (2023-2024)

Sponsor: Rep. McMorris Rodgers, Cathy [R-WA-5] (Introduced 06/25/2024)
Committees: House - Energy and Commerce
Latest Action: House - 06/25/2024 Referred to the House Committee on Energy and Commerce. (All Actions)
Tracker: Introduced

Listen

There is one version of the bill. **Text available as:** XML/HTML | Download XML (291KB) | TXT (251KB) | PDF (499KB)

Shown Here:
Introduced in House (06/25/2024)

118TH CONGRESS
2D SESSION

H. R. 8818

To provide Americans with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 25, 2024

Mrs. RODGERS of Washington (for herself, Mr. PALLONE, Mr. BILIRAKIS, and Ms. SCHAKOWSKY) introduced the following bill; which was referred to the Committee on Energy and Commerce

A BILL

To provide Americans with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "American Privacy Rights Act of 2024".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

TITLE I—AMERICAN PRIVACY RIGHTS

SEC. 101. DEFINITIONS.

In this title:

(1) AFFIRMATIVE EXPRESS CONSENT.—

(A) IN GENERAL.—The term "affirmative express consent" means an affirmative act by an individual that—

(i) clearly communicates the authorization of the individual for an act or practice; and

(ii) is provided in response to a specific request from a covered entity, or a service provider on behalf of a covered entity, that meets the requirements of subparagraph (B).

(B) REQUEST REQUIREMENTS.—The requirements of this subparagraph with respect to a request are the following:

(i) The request is provided to the individual in a clear and conspicuous standalone disclosure.

(ii) The request includes a description of each act or practice for which the consent of the individual is sought and—

(I) clearly distinguishes between an act or practice that is necessary, proportionate, and limited to fulfill a request of the individual and an act or practice that is for another purpose;

(II) clearly states the specific categories of covered data that the covered entity shall collect, process, retain, or transfer under each such act or practice; and

(III) is written in easy-to-understand language and includes a prominent heading that would enable a reasonable individual to identify and understand each such act or practice.

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

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

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

(vi) The option to refuse consent is at least as prominent as the option to provide consent, and the option to refuse consent takes no more than 1 additional step as compared to the number of steps necessary to provide consent.

(vii) With respect to affirmative express consent sought for the collection, processing, retention, or transfer of biometric information or genetic information, the request includes the length of time the covered entity or service provider intends to retain the biometric information or genetic information or, if it is not possible to identify the length of time, the criteria used to determine the length of time the covered entity or service provider intends to retain the biometric information or genetic information.

(C) EXPRESS CONSENT REQUIRED.—Affirmative express consent to an act or practice may not be inferred from the inaction of an individual or the continued use by an individual of a service or product provided by an entity.

(D) WITHDRAWAL OF AFFIRMATIVE EXPRESS CONSENT.—

(i) IN GENERAL.—A covered entity shall provide an individual with a means to withdraw affirmative express consent previously provided by the individual.

(ii) REQUIREMENTS.—The means to withdraw affirmative express consent described in clause (i) shall be—

(I) clear and conspicuous; and

(II) as easy for a reasonable individual to use as the mechanism by which the individual provided affirmative express consent.

(E) CHILDREN AND TEENS.—If a covered entity has knowledge that —

(i) an individual is a child, only a parent of the child may provide affirmative express consent on behalf of the child; or

(ii) an individual is a teen, a parent or the teen may provide affirmative express consent on behalf of the teen.

(2) BIOMETRIC INFORMATION.—

(A) IN GENERAL.—The term "biometric information" means any covered data that allows or confirms the unique identification or verification of an individual and is generated from the measurement or processing of unique biological, physical, or physiological characteristics, including—

(i) fingerprints;

(ii) voice prints;

(iii) iris or retina imagery scans;

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

(v) gait.

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

(i) a digital or physical photograph;

(ii) an audio or video recording; or

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

(3) CHILD.—The term "child" means an individual under the age of 13.

(4) CLEAR AND CONSPICUOUS.—The term "clear and conspicuous" means, with respect to a disclosure, that the disclosure is difficult to miss and easily understandable by ordinary consumers.

(5) COARSE GEOLOCATION INFORMATION.—The term "coarse geolocation information" means information that reveals the present physical location of an individual or device identified by a unique persistent identifier at the ZIP Code attribution level (except, if a geographic area attributed to a ZIP Code is equal to or less than the area of a circle with a radius of 1,850 feet or less, at a level greater than a geographic area equal to the area of a circle with a radius of 1,850 feet).

(6) COLLECT.—The term "collect" means, with respect to covered data, to buy, rent, gather, obtain, receive, access, or otherwise acquire the covered data by any means.

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

(8) COMMON BRANDING.—The term "common branding" means a name, service mark, or trademark that is shared by 2 or more entities.

(9) CONNECTED DEVICE.—The term "connected device" means a device that is capable of connecting to the internet.

(10) CONTEXTUAL ADVERTISING.—The term "contextual advertising" means displaying or presenting an advertisement that—

(A) does not vary based on the identity of the individual recipient; and

(B) is based solely on—

(i) the content of a webpage or online service;

(ii) a specific request of the individual for information or feedback; or

(iii) coarse geolocation information.

(11) 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.

(12) 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 1 or more individuals.

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

(i) de-identified data;

(ii) employee information;

(iii) publicly available information;

(iv) inferences made exclusively from multiple independent sources of publicly available information, if such inferences—

(I) do not reveal information about an individual that meets the definition of the term "sensitive covered data" with respect to the individual; and

(II) are not combined with covered data;

(v) information in the collection of a library, archive, or museum, if —

(I) the collection is—

(aa) open to the public or routinely made available to researchers who are not affiliated with the library, archive, or museum; and

(bb) composed of lawfully acquired materials with respect to which all licensing conditions are met; and

(II) the library, archive, or museum has—

(aa) a public service mission; and

(bb) trained staff or volunteers to provide professional services normally associated with libraries, archives, or museums; or

(vi) on-device data.

(13) COVERED ENTITY.—

(A) IN GENERAL.—The term "covered entity" means any entity that, alone or jointly with others, determines the purposes and means of collecting, processing, retaining, 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 title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.); or

(iii) is an organization not organized to carry on business for its own profit or that of its members.

(B) INCLUSION.—The term "covered entity" includes any entity that controls, is controlled by, or is under common control with another covered entity.

(C) EXCLUSIONS.—The term "covered entity" does not include—

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

(ii) an entity that is collecting, processing, retaining, or transferring covered data on behalf of a Federal, State, Tribal, or local government entity, to the extent that such entity is acting as a service provider to the government entity;

(iii) a small business;

(iv) an individual acting at their own direction and in a non-commercial context;

(v) the National Center for Missing and Exploited Children; or

(vi) except with respect to requirements under section 109, a nonprofit organization whose primary mission is to prevent, investigate, or deter fraud, to train anti-fraud professionals, or to educate the public about fraud, including insurance fraud, securities fraud, and financial fraud, to the extent the organization collects, processes, retains, or transfers covered data in furtherance of such primary mission.

(D) NONAPPLICATION TO SERVICE PROVIDERS.—An entity may not be considered to be a "covered entity" for the purposes of this title, insofar as the entity is acting as a service provider.

(14) COVERED HIGH-IMPACT SOCIAL MEDIA COMPANY.—

(A) IN GENERAL.—The term "covered high-impact social media company" means a covered entity that provides any internet-accessible platform that—

(i) generates $3,000,000,000 or more in global annual revenue, including the revenue generated by any affiliate of such covered entity;

(ii) has 300,000,000 or more global monthly active users for not fewer than 3 of the preceding 12 months; and

(iii) constitutes an online product or service that is primarily used by users to access or share user-generated content.

(B) TREATMENT OF CERTAIN SERVICES AND APPLICATIONS.—A service or application may not be considered to constitute an online product or service described in subparagraph (A)(iii) solely on the basis of providing any of the following:

(i) Email.

(ii) Career or professional development networking opportunities.

(iii) Reviews of products, services, events, or destinations.

(iv) A platform for use in a public or private school under the direction of the school.

(v) File collaboration.

(vi) Cloud storage.

(vii) Closed video or audio communications services.

(viii) A wireless messaging service, including such a service provided through short messaging service or multimedia messaging service protocols, that is not a component of, or linked to, a platform of a covered high-impact social media company, if the predominant or exclusive function is direct messaging consisting of the transmission of text, photos, or videos that are sent by electronic means, and if messages are transmitted from the sender to a recipient and are not posted within a platform of a covered high-impact social media company or publicly.

(15) COVERED MINOR.—The term "covered minor" means an individual under the age of 17.

(16) DARK PATTERNS.—The term "dark patterns" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.

(17) DATA BROKER.—

(A) IN GENERAL.—The term "data broker" 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.

(B) PRINCIPAL SOURCE OF REVENUE.—For purposes of this paragraph, the term "principal source of revenue" means, for the prior 12-month period—

(i) revenue that constitutes greater than 50 percent of all revenue of the covered entity during such period; or

(ii) revenue obtained from processing and 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) NON-APPLICATION TO SERVICE PROVIDERS.—The term "data broker" does not include an entity to the extent that such entity is acting as a service provider.

(18) DE-IDENTIFIED DATA.—

(A) IN GENERAL.—The term "de-identified data" means information that cannot reasonably be used to infer or derive the identity of an individual, and does not identify and is not linked or reasonably linkable to an individual or a device that identifies or is linked or reasonably linkable to an individual, regardless of whether the information is aggregated, if the relevant covered entity or service provider—

(i) takes reasonable physical, administrative, and 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;

(ii) publicly commits in a clear and conspicuous manner to—

(I) process, retain, or transfer the information solely in a de-identified form without any reasonable means for re-identification; and

(II) not attempt to re-identify the information with any individual or device that identifies or is linked or reasonably linkable to an individual, except as necessary, limited, and proportionate to test the effectiveness of the measures described in clause (i); and

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

(I) comply with clauses (i) and (ii) with respect to the information; and

(II) require that such contractual obligations be included contractually in all subsequent instances in which the information may be received.

(B) HEALTH INFORMATION.—The term "de-identified data" includes health information (as defined in section 1171 of the Social Security Act (42 U.S.C. 1320d)) that has been de-identified in accordance with section 164.514(b) of title 45, Code of Federal Regulations, except that if such

information is subsequently provided to an entity that is not an entity subject to parts 160 and 164 of such title 45, such entity shall comply with clauses (ii) and (iii) of subparagraph (A) for the information to be considered de-identified under this title.

(19) 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.

(20) DEVICE.—The term "device" means any electronic equipment capable of collecting, processing, retaining, or transferring covered data that is used by 1 or more individuals, including a connected device or a portable connected device.

(21) DIRECT MAIL TARGETED ADVERTISING.—The term "direct mail targeted advertising" means advertising or marketing using third-party data through a direct communication with an individual via direct mail.

(22) DISABILITY.—The term "disability" has the meaning given such term in section 3 of the Americans with Disabilities Act of 1990 (42 U.S.C. 12102).

(23) EMAIL TARGETED ADVERTISING.—The term "email targeted advertising" means advertising or marketing using third-party data through a direct communication with an individual via email.

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

(25) EMPLOYEE INFORMATION.—The term "employee information" means information, including biometric information or genetic information—

(A) about an individual related to the course of employment or application for employment of the individual (including on a contract or temporary basis), if such information is collected, retained, processed, or transferred by the employer or the service provider of the employer solely for purposes necessary for the employment or application of the individual;

(B) that is emergency contact information for an individual who is an employee or job applicant of an employer, if such information is collected, retained, processed, or transferred by the employer or the service provider of the employer solely for the purpose of having an emergency contact for such individual on file; or

(C) about an individual who is an employee or former employee of an employer, or a relative, dependent, or beneficiary of the employee or former employee, and collected, retained, processed, or transferred for the purpose of administering benefits, including enrollment and disenrollment for benefits, to which the employee, former employee, relative, dependent, or beneficiary is entitled on the basis of the employment of the employee or former employee with the employer, if such information is collected, retained, processed, or transferred by the employer or the service provider of the employer solely for the purpose of administering such benefits.

(26) ENTITY.—The term "entity" means an individual, a trust, a partnership, an association, an organization, a company, and a corporation.

(27) EXECUTIVE AGENCY.—The term "Executive agency" has the meaning given such term in section 105 of title 5, United States Code.

(28) FEDERATED NONPROFIT ORGANIZATION.—The term "federated nonprofit organization" means a network or system of 2 or more entities, described in section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from taxation under section 501(a) of such Code, that share common branding.

(29) FIRST PARTY.—The term "first party"—

(A) means a consumer-facing covered entity with which a consumer intends and expects to interact; and

(B) includes any entities with which the covered entity shares common branding.

(30) FIRST-PARTY ADVERTISING.—

(A) IN GENERAL.—The term "first-party advertising" means advertising or marketing by a first party using the first-party data of the first party and not other forms of covered data and carried out—

(i) through direct communications with an individual, such as direct mail, email (subject to the CAN-SPAM Act of 2003 (15 U.S.C. 7701 et seq.) and the regulations promulgated under such Act), or text message communications (subject to section 227 of the Communications Act of 1934 (47 U.S.C. 227) and the regulations promulgated under such section); or

(ii) entirely—

(I) in a physical location operated by the first party;

(II) in the case of a first party that is not a covered high-impact social media company, on a website, online service, online application, or mobile application operated by the first party, through display or presentation of an online advertisement that promotes a product or service (whether offered by the first party or not offered by the first party) to an individual or device identified by a unique persistent identifier, or group of individuals or devices identified by unique persistent identifiers; or

(III) in the case of a first party that is a covered high-impact social media company, on a website, online service, online application, or mobile application operated by the first party, through display or presentation of an online advertisement that promotes a product or service offered by the first party to an individual or device identified by a unique persistent identifier, or group of individuals or devices identified by unique persistent identifiers.

(B) EXCLUSION.—The term "first-party advertising" does not include contextual advertising.

(31) FIRST-PARTY DATA.—The term "first-party data" means covered data collected directly from an individual by a first party, including based on a visit by the individual to or use by the individual of a physical location, website, online service, online application, or mobile application operated by the first party.

(32) GENETIC INFORMATION.—The term "genetic information" means any covered data, regardless of format, that concerns the genetic characteristics of an identified or identifiable individual, including—

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

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

(33) HEALTH INFORMATION.—The term "health information" means information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or health condition, status, or treatment of an individual, including the precise geolocation information of such treatment.

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

(35) KNOWLEDGE.—

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

(B) RULE OF CONSTRUCTION.—For purposes of enforcing this title or a regulation promulgated under this title, a determination as to whether a covered entity has knowledge fairly implied on the basis of objective circumstances that an individual is a child, teen, or covered minor 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 individual is a child, teen, or covered minor. Nothing in this title, including a determination described in the preceding sentence, may be construed to require a covered entity to—

(i) affirmatively collect any covered data with respect to the age of a child, teen, or covered minor that the covered entity is not already collecting in the normal course of business; or

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

(C) COMMISSION GUIDANCE.—

(i) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Commission shall issue guidance to provide information, including best practices and examples, for covered entities to use in understanding whether a covered entity has knowledge fairly implied on the basis of objective circumstances that an individual is a child, teen, or covered minor.

(ii) LIMITATION.—No guidance issued by the Commission under clause (i) confers any rights on any person, State, or locality, or operates to bind the Commission or any person, State, or locality to the approach recommended in such guidance. Any enforcement action brought pursuant to this title by the Commission, or by the attorney general of a State, the chief consumer protection officer of a State, or an officer or office of a State authorized to enforce privacy or data security laws applicable to covered entities or service providers, shall allege a specific violation of a provision of this title, and the Commission or the attorney general, chief consumer protection officer, or other authorized officer or office of the State, as applicable, may not base an enforcement action on, or as applicable execute a consent order based on, practices that are alleged to be inconsistent with any such guidance, unless the practices allegedly violate this title.

(36) 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, had an annual gross revenue of not less than $250,000,000 and, subject to subparagraph (B), collected, processed, retained, or transferred—

(i) the covered data of—

(I) more than 5,000,000 individuals;

(II) more than 15,000,000 portable connected devices that identify or are linked or reasonably linkable to 1 or more individuals; or

(III) more than 35,000,000 connected devices that identify or are linked or reasonable linkable to 1 or more individuals; or

(ii) the sensitive covered data of—

(I) more than 200,000 individuals;

(II) more than 300,000 portable connected devices that identify or are linked or reasonable linkable to 1 or more individuals; or

(III) more than 700,000 connected devices that identify or are linked or reasonably linkable to 1 or more individuals.

(B) EXCLUSIONS.—For the purposes of subparagraph (A), a covered entity or service provider may not be considered a large data holder solely on the basis of collecting, processing, retaining, or transferring to a service provider—

(i) personal mailing or email addresses;

(ii) personal telephone numbers;

(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

(iv) in the case of a covered entity that is a seller of goods or services (other than an entity that facilitates payment, such as a bank, credit card processor, mobile payment system, or payment platform), credit, debit, or mobile payment information necessary and used to initiate, render, bill for, finalize, complete, or otherwise facilitate payments for such goods or services.

(C) DEFINITION OF ANNUAL GROSS REVENUE.—For the purposes of subparagraph (A), the term "annual gross revenue", with respect to a covered entity or service provider—

(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.

(37) MARKET RESEARCH.—The term "market research" means the collection, processing, retention, or transfer of covered data, with affirmative express consent, that is necessary, proportionate, and limited to measure and analyze the market or market trends of products, services, advertising, or ideas, if the covered data is not—

(A) integrated into any product or service;

(B) otherwise used to contact any individual or device of an individual; or

(C) used for targeted advertising or to otherwise market to any individual or device of an individual.

(38) MATERIAL CHANGE.—The term "material change" means, with respect to treatment of covered data, a change by an entity that would likely affect the decision of an individual to engage with and provide covered data to the entity, including providing affirmative express consent for, or opting out of, the collection, processing, retention, or transfer of covered data pertaining to such individual.

(39) 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.

(40) ON-DEVICE DATA.—

(A) IN GENERAL.—The term "on-device data" means data collected, retained, and processed solely on the device of an individual.

(B) LIMITATION.—Data collected, retained, and processed solely on the device of an individual may be considered "on-device data" only if—

(i) such data is not transferred by a covered entity or service provider;

(ii) the relevant covered entity clearly and conspicuously provides the device owner with controls that allow the owner to access, correct, delete, and export such data consistent with the rights provided with respect to covered data pursuant to section 105;

(iii) the relevant covered entity provides easy-to-understand instructions on how the device owner can access such controls; and

(iv) the relevant covered entity establishes, implements, and maintains reasonable data security practices, consistent with section 109, to protect—

(I) the confidentiality, integrity, and availability of the on-device data; and

(II) on device data against unauthorized access.

(41) ONLINE ACTIVITY PROFILE.—The term "online activity profile" means covered data that identifies the online activities of an individual (or a device linked or reasonably linkable to an individual) over time and across third-party websites, online services, online applications, or mobile applications that do not share common branding and that is collected, processed, retained, or transferred for the purpose of evaluating, analyzing, or predicting the behaviors or characteristics of an individual.

(42) 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.

(43) PARENT.—The term "parent" means a legal guardian.

(44) PORTABLE CONNECTED DEVICE.—The term "portable connected device" means a portable device that is capable of connecting to the internet over

a wireless connection, including a smartphone, tablet computer, laptop computer, smartwatch, or similar portable device.

(45) PRECISE GEOLOCATION INFORMATION.—

(A) IN GENERAL.—The term "precise geolocation information" means information that reveals the past or present physical location of an individual or device with sufficient precision to identify the location of such individual or device within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet or less.

(B) EXCLUSIONS.—The term "precise geolocation information" does not include information derived solely from—

(i) a digital or physical photograph;

(ii) an audio or visual recording; or

(iii) metadata associated with a digital or physical photograph or an audio or visual recording that cannot be linked to an individual.

(46) PROCESS.—The term "process" means, with respect to covered data, any operation or set of operations performed on the covered data, including analyzing, organizing, structuring, using, modifying, or otherwise handling the covered data.

(47) PUBLICLY AVAILABLE INFORMATION.—

(A) IN GENERAL.—The term "publicly available information" means any information that a covered entity has a reasonable basis to believe has been lawfully made available to the general public by—

(i) Federal, State, or local government records, if the covered entity collects, processes, retains, 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 can log in to the website or online service; or

(iv) a disclosure to the general public that is required to be made by Federal, State, or local law.

(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 to whom the information pertains has restricted the information to a specific audience or maintained a default setting that restricts the information to a specific audience.

(ii) BUSINESS CONTACT INFORMATION.—The term "publicly available information" includes business contact information of an individual acting in a business or professional context that is made available on a website or online service made available to all members of the public, including the name, position or title, business telephone number, business email address, or business address of the individual.

(iii) OTHER LIMITATIONS.—The term "publicly available information" does not include—

(I) any obscene visual depiction (as such term is used in section 1460 of title 18, United States Code);

(II) derived data from publicly available information that reveals information about an individual that meets the definition of the term "sensitive covered data";

(III) biometric information;

(IV) genetic information, unless made publicly available by the individual to whom the information pertains by a means described in clause (ii) or (iii) of subparagraph (A);

(V) covered data that is created through the combination of covered data with publicly available information;

(VI) intimate images, authentic or computer-generated, known to be nonconsensual; or

(VII) sensitive covered data made available by a data broker.

(48) RETAIN.—The term "retain" means, with respect to covered data, to store, maintain, save, or otherwise keep such data, regardless of format.

(49) SENSITIVE COVERED DATA.—

(A) IN GENERAL.—The term "sensitive covered data" means the following forms of covered data:

(i) A government-issued identifier, including 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 condition, status, or treatment of an individual.

(iii) Genetic information.

(iv) A financial account number, debit card number, credit card number, or any required security or access code, password, or credentials allowing access to any such account or card, except that the last four digits of an account number, debit card number, or credit card number may not be considered sensitive covered data.

(v) Biometric information.

(vi) Precise geolocation information.

(vii) The private communications of an individual (such as voicemails, or other voice or video communications, emails, texts, direct messages, or mail) or information identifying the parties to such communications, information contained in telephone bills, and any information that pertains to the transmission of private voice or video communications, including numbers called, numbers from which calls were placed, the time calls were made, call duration, and location information of the parties to the call, unless the relevant covered entity or service provider is an intended recipient of the communication.

(viii) Unencrypted or unredacted account or device log-in credentials.

(ix) Information revealing the sexual behavior of an individual in a manner inconsistent with the reasonable expectation of the individual regarding disclosure of such information.

(x) Calendar information, address book information, phone, text, or electronic logs, photographs, audio recordings, or videos intended for private use.

(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 extent or content of the access, viewing, or other use by an individual of any video programming (as defined in section 713(h)(2) of the Communications Act of 1934 (47

U.S.C. 613(h)(2))), including programming provided by a provider of broadcast television service, cable service, satellite service, or streaming media service, but only with regard to the transfer of such information to a third party (excluding any such information used solely for transfers for independent video measurement).

(xiii) Information collected by a covered entity that is not a provider of a service described in clause (xii) that reveals the video content requested or selected by an individual (excluding any such information used solely for transfers for independent video measurement).

(xiv) Information revealing the race, ethnicity, national origin, religion, or sex of an individual in a manner inconsistent with the reasonable expectation of the individual regarding disclosure of such information.

(xv) An online activity profile.

(xvi) Information about a covered minor.

(xvii) Information that reveals the status of an individual as a member of the Armed Forces.

(xviii) Neural data.

(xix) Any other covered data collected, processed, retained, or transferred for the purpose of identifying a type of information described in any of clauses (i) through (xviii).

(B) THIRD PARTY.—For the purposes of subparagraph (A)(xii), the term "third party" does not include an entity that—

(i) is related by common ownership or corporate control to the provider of broadcast television service or streaming media service; and

(ii) provides video programming as described in such subparagraph.

(50) SERVICE PROVIDER.—

(A) IN GENERAL.—The term "service provider" means an entity that collects, processes, retains, or transfers covered data for the purpose of performing 1 or more services or functions on behalf of, and at the direction of—

(i) a covered entity or another service provider; or

(ii) a Federal, State, Tribal, or local government entity.

(B) RULE OF CONSTRUCTION.—

(i) IN GENERAL.—An entity is a covered entity and not a service provider with respect to a specific collecting, processing, retaining, or transferring of covered data, if the entity, alone or jointly with others, determines the purposes and means of the specific collecting, processing, retaining, or transferring of data.

(ii) INSTRUCTIONS.—An entity that is not limited in its collecting, processing, retaining, or transferring of covered data pursuant to the instructions of a covered entity, another service provider, or a Federal, State, Tribal, or local government entity, or that fails to adhere to such instructions, is a covered entity and not a service provider with respect to a specific collecting, processing, retaining, or transferring of such data. If a service provider begins, alone or jointly with others, determining the purposes and means of collecting, processing, retaining, or transferring covered data, the entity is a covered entity with respect to such data.

(iii) CONTEXT REQUIRED.—Whether an entity is a covered entity or a service provider depends on the facts surrounding how, and the context in which, data is collected, processed, retained, or transferred.

(51) SMALL BUSINESS.—

(A) IN GENERAL.—The term "small business" means an entity (including any affiliate of the entity)—

(i) that has average annual gross revenues for the period of the 3 preceding calendar years (or for the period during which the entity has been in existence, if such period is less than 3 calendar years) not exceeding $40,000,000, indexed to the Producer Price Index reported by the Bureau of Labor Statistics;

(ii) that, on average for the period described in clause (i), did not annually collect, process, retain, or transfer the covered data of more than 200,000 individuals for any purpose other than initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product; and

(iii) that did not, during the period described in clause (i), transfer covered data to a third party in exchange for revenue or anything of

value, except for purposes of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product or facilitating web analytics that are not used to create an online activity profile.

(B) NONPROFIT REVENUE.—For purposes of subparagraph (A)(i), the term "revenue", as such term relates to any entity that is not organized to carry on business for its own profit or that of its members, means the gross receipts the entity received, in whatever form from all sources, without subtracting any costs or expenses, and includes contributions, gifts, grants (except for grants from the Federal Government), dues or other assessments, income from investments, or proceeds from the sale of real or personal property.

(52) STATE.—The term "State" means each of the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands of the United States, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

(53) SUBSTANTIAL PRIVACY HARM.—The term "substantial privacy harm" means—

(A) any alleged financial harm of not less than $10,000; or

(B) any alleged physical or mental harm to an individual that involves—

(i) treatment by a licensed, credentialed, or otherwise bona fide health care provider, hospital, community health center, clinic, hospice, or residential or outpatient facility for medical, mental health, or addiction care; or

(ii) physical 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.

(54) TARGETED ADVERTISING.—The term "targeted advertising"—

(A) means displaying or presenting an online advertisement to an individual or to a device identified by a unique persistent identifier (or to a group of individuals or devices identified by unique persistent identifiers), if the advertisement is selected based, in whole or in part, on known or predicted preferences or interests associated with the individual or device;

(B) includes—

(i) an online advertisement by a covered high-impact social media company for a product or service that is not a product or service offered by the covered high-impact social media company; and

(ii) an online advertisement for a product or service based on the previous interaction of an individual or a device identified by a unique persistent identifier with such product or service on a website or online service that does not share common branding or affiliation with the website or online service displaying or presenting the advertisement; and

(C) excludes contextual advertising and first-party advertising.

(55) TEEN.—The term "teen" means an individual 13 years of age or older, but under the age of 17.

(56) THIRD PARTY.—The term "third party"—

(A) means any entity that—

(i) receives covered data from another entity that is not the individual to whom the data pertains; and

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

(B) does not include an entity that collects covered data from another entity if the 2 entities are—

(i) related by common ownership or corporate control; or

(ii) nonprofit entities that are part of the same federated nonprofit organization.

(57) THIRD-PARTY DATA.—The term "third-party data" means covered data that has been transferred to a third party.

(58) TRANSFER.—The term "transfer" means, with respect to covered data, to disclose, release, share, disseminate, make available, sell, rent, or license the covered data (orally, in writing, electronically, or by any other means) for consideration of any kind or for a commercial purpose.

(59) UNIQUE PERSISTENT IDENTIFIER.—

(A) IN GENERAL.—The term "unique persistent identifier" means a technologically created identifier to the extent that such identifier is reasonably linkable to an individual or a device that identifies or is linked or reasonably linkable to 1 or more individuals, including device identifiers,

Internet Protocol addresses, cookies, beacons, pixel tags, mobile ad identifiers or similar technology customer numbers, unique pseudonyms, user aliases, telephone numbers, or other forms of persistent or probabilistic identifiers that are linked or reasonably linkable to 1 or more individuals or devices.

(B) EXCLUSION.—The term "unique persistent identifier" does not include an identifier assigned by a covered entity for the sole purpose of giving effect to the exercise of affirmative express consent or opt out by an individual with respect to the collecting, processing, retaining, and transfer of covered data or otherwise limiting the collecting, processing, retaining, or transfer of covered data.

(60) WIDELY DISTRIBUTED MEDIA.—

(A) IN GENERAL.—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.

(B) EXCLUSION.—The term "widely distributed media" does not include an obscene visual depiction (as such term is used in section 1460 of title 18, United States Code).

SEC. 102. DATA MINIMIZATION.

(a) IN GENERAL.—A covered entity may not collect, process, retain, or transfer covered data of an individual or direct a service provider to collect, process, retain, or transfer covered data of an individual beyond what is necessary, proportionate, and limited—

(1) to provide or maintain—

(A) a specific product or service requested by the individual to whom the data pertains, including any associated routine administrative, operational, or account-servicing activity, such as billing, shipping, delivery, storage, or accounting; or

(B) a communication, that is not an advertisement, by the covered entity to the individual reasonably anticipated within the context of the relationship; or

(2) for a purpose expressly permitted under subsection (d).

(b) ADDITIONAL PROTECTIONS FOR SENSITIVE COVERED DATA.—Subject to subsection (a), a covered entity may not transfer sensitive covered data to a third party or direct a service provider to transfer sensitive covered data to a third party without the

affirmative express consent of the individual to whom such data pertains, unless for a purpose permitted by paragraph (2), (3), (4), (5), (6), (8), (9), (11), (12), or (13) of subsection (d).

(c) ADDITIONAL PROTECTIONS FOR BIOMETRIC INFORMATION AND GENETIC INFORMATION.—

(1) COLLECTION.—Subject to subsection (a), a covered entity may not collect biometric information or genetic information or direct a service provider to collect biometric information or genetic information without the affirmative express consent of the individual to whom such information pertains.

(2) PROCESSING.—Subject to subsection (a), a covered entity may not process biometric information or genetic information or direct a service provider to process biometric information or genetic information without the affirmative express consent of the individual to whom such information pertains, unless for a purpose permitted by paragraph (2), (3), or (4) of subsection (d).

(3) RETENTION.—Subject to subsection (a), a covered entity may not retain biometric information or direct a service provider to retain biometric information beyond the point at which the purpose for which an individual provided affirmative express consent under paragraph (1) has been satisfied or beyond the date that is 3 years after the date of the last interaction of the individual with the covered entity or service provider, whichever occurs first, unless for a purpose permitted under paragraph (2), (3), or (4) of subsection (d).

(4) TRANSFER.—

(A) AFFIRMATIVE EXPRESS CONSENT REQUIRED.—Subject to subsection (a), a covered entity may not transfer biometric information or genetic information to a third party or direct a service provider to transfer biometric information or genetic information to a third party without the affirmative express consent of the individual to whom such information pertains, unless for a purpose permitted by paragraph (2), (3), or (4) of subsection (d).

(B) NO TRANSFER FOR PAYMENT OR OTHER VALUABLE CONSIDERATION.—A covered entity may not transfer biometric information or genetic information to a third party, or direct a service provider to transfer biometric information or genetic information to a third party, for payment or other valuable consideration (regardless of the purpose of the transfer, including a purpose described in subparagraph (A)).

(d) PERMITTED PURPOSES.—Subject to the requirements in subsections (b) and (c), a covered entity may collect, process, retain, or transfer or direct a service provider to collect, process, retain, or transfer covered data for the following purposes, if the

covered entity or service provider can demonstrate that the collection, processing, retention, or transfer is necessary, proportionate, and limited to such purpose:

(1) To protect data security as described in section 109, protect against spam, or protect and maintain networks and systems, including through diagnostics, debugging, and repairs.

(2) To comply with a legal obligation imposed by a Federal, State, Tribal, or local law that is not preempted by this title.

(3) To investigate, establish, prepare for, exercise, or defend cognizable legal claims of the covered entity or service provider.

(4) To transfer covered data to a Federal, State, Tribal, or local law enforcement agency pursuant to a lawful warrant, administrative subpoena, or other form of lawful process.

(5) To effectuate a product recall pursuant to Federal or State law, or to fulfill a warranty.

(6) To conduct market research.

(7) With respect to covered data previously collected in accordance with this title, to process the covered data such that the covered data becomes de-identified data, including in order to—

(A) develop or enhance a product or service of the covered entity or service provider;

(B) conduct research or analytics to improve a product or service of the covered entity or service provider;

(C) conduct research to investigate, establish, or improve the effectiveness or safety of medical products, including drugs, biologics, and medical devices;

(D) enable the effective delivery and administration of health care products and treatments to patients, in compliance with Federal regulations; or

(E) monitor the safety and efficacy of health care products and services administered to patients, in compliance with Federal regulations.

(8) To transfer assets to a third party in the context of a merger, acquisition, bankruptcy, or similar transaction, with respect to which the third party assumes control, in whole or in part, of the assets of the covered entity, but only if the

covered entity, in a reasonable time prior to such transfer, provides each affected individual with—

(A) a notice describing such transfer, including the name of the entity or entities receiving the covered data of the individual and the privacy policies of such entity or entities as described in section 104; and

(B) a reasonable opportunity to—

(i) withdraw any previously provided consent in accordance with the requirements of affirmative express consent under this title related to the covered data of the individual; and

(ii) request the deletion of the covered data of the individual, as described in section 105.

(9) With respect to a covered entity or service provider that is a telecommunications carrier or a provider of a mobile service, interconnected VoIP service, or non-interconnected VoIP service (as such terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153)), to provide call location information in a manner described in subparagraph (A) or (C) of section 222(d)(4) of such Act (47 U.S.C. 222(d)(4)).

(10) To prevent, detect, protect against, investigate, or respond to fraud, excluding the transfer of covered data for payment or other valuable consideration to a government entity.

(11) To prevent, detect, protect against, investigate, or respond to an ongoing or imminent security incident relating to network security or physical security, including an intrusion or trespass, medical alert or request for a medical response, fire alarm or request for a fire response, or access control.

(12) To prevent, detect, protect against, investigate, or respond to an imminent or ongoing public safety incident (such as a mass casualty event, natural disaster, or national security incident), excluding the transfer of covered data for payment or other valuable consideration to a government entity.

(13) Except with respect to health information, to prevent, detect, protect against, investigate, or respond to criminal activity or harassment, excluding the transfer of covered data for payment or other valuable consideration to a government entity.

(14) Except with respect to sensitive covered data, and only with respect to covered data previously collected in accordance with this title, to process or transfer such data to provide first-party advertising or contextual advertising or to measure and report on marketing performance or media performance by the covered entity, including processing or transferring covered data for measurement

and reporting of frequency, attribution, and performance, including by independent entities, except that this paragraph does not permit the processing or transfer of covered data for first-party advertising to a covered minor as prohibited by section 120.

(15) Except with respect to sensitive covered data, and only with respect to covered data previously collected in accordance with this title, to process or transfer such data to provide targeted advertising, direct mail targeted advertising, or email targeted advertising (subject to the CAN-SPAM Act of 2003 (15 U.S.C. 7701 et seq.) and the regulations promulgated under such Act) or to measure and report on marketing performance or media performance, including processing or transferring covered data for measurement and reporting of frequency, attribution, and performance, including by independent entities, except that this paragraph does not permit the processing or transfer of covered data for targeted advertising to an individual who has opted out of targeted advertising pursuant to section 106 or to a covered minor as prohibited by section 120.

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

(A) is in the public interest;

(B) adheres to all relevant laws and regulations governing such research, including regulations for the protection of human subjects, if applicable;

(C) limits transfers to third parties of sensitive covered data to only those transfers necessary, proportionate, and limited to carry out the research; and

(D) prohibits the transfer of covered data to a data broker.

(17) To conduct medical research in compliance with part 46 of title 45, Code of Federal Regulations, or parts 50 and 56 of title 21, Code of Federal Regulations.

(e) GUIDANCE.—Not later than 180 days after the date of the enactment of this Act, the Commission shall issue guidance regarding what is necessary, proportionate, and limited to comply with this section.

(f) JOURNALISM.—Nothing in this title may be construed to limit or diminish journalism, including gathering, preparing, collecting, photographing, recording, writing, editing, reporting, or investigating news or information that concerns local, national, or international events or other matters of public interest for dissemination to the public.

SEC. 103. PRIVACY BY DESIGN.

(a) In General.—Each covered entity and 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, retention, and transferring of covered data.

(b) Requirements.—The policies, practices, and procedures required by subsection (a) shall—

(1) identify, assess, and mitigate privacy risks related to covered minors (including, if applicable, in a manner that considers the developmental needs of different age ranges of covered minors), individuals living with disabilities, and individuals over the age of 65;

(2) mitigate privacy risks related to the products and services of the covered entity or 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 the covered entity or service provider; and

(3) implement reasonable internal training and safeguards to promote compliance with this title and to mitigate privacy risks, taking into account the role of the covered entity or service provider and the information available to the covered entity or service provider.

(c) Factors To Consider.—The policies, practices, and procedures established by a covered entity or service provider under subsection (a) shall align with, as applicable —

(1) 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, or data broker, taking into account the role of the covered entity or service provider and the information available to the covered entity or service provider;

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

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

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

(5) state-of-the-art administrative, technological, and organizational measures that, by default, serve the purpose of protecting the privacy and security of

covered data as required by this title; and

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

(d) COMMISSION GUIDANCE.—Not later than 1 year after the date of the enactment of this Act, the Commission shall issue guidance with respect to what constitutes reasonable policies, practices, and procedures as required by subsection (a). In issuing such guidance, the Commission shall consider unique circumstances applicable to nonprofit organizations, service providers, and data brokers.

SEC. 104. TRANSPARENCY.

(a) IN GENERAL.—Each covered entity and service provider shall make publicly available a clear and conspicuous, not misleading, and easy-to-read privacy policy that provides a detailed and accurate representation of the data collection, processing, retention, and transfer activities of the covered entity or service provider.

(b) CONTENT OF PRIVACY POLICY.—The privacy policy required under subsection (a) shall include, at a minimum, the following:

(1) The identity and the contact information of—

(A) the covered entity or service provider to which the privacy policy applies, including a point of contact and a monitored email address or other monitored online contact mechanism, as applicable, specific to data privacy and data security inquiries; and

(B) any affiliate within the same corporate structure as the covered entity or service provider, to which the covered entity or service provider may transfer data, that—

(i) is not under common branding with the covered entity or service provider; or

(ii) has different contact information than the covered entity or service provider.

(2) With respect to the collection, processing, and retention of covered data—

(A) the categories of covered data the covered entity or service provider collects, processes, or retains; and

(B) the processing purposes for each such category of covered data.

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

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

(B) the name of each data broker to which the covered entity or service provider transfers covered data; and

(C) the purposes for which such data is transferred.

(4) The length of time the covered entity or service provider intends to retain each category of covered data or, if it is not possible to identify the length of time, the criteria used to determine the length of time the covered entity or service provider intends to retain each category of covered data.

(5) A prominent description of how an individual may exercise the rights, as applicable, of the individual under this title.

(6) A description of how the covered entity treats data collected from covered minors differently than data collected from other individuals, if the covered entity has knowledge that the covered entity has collected data from covered minors.

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

(8) The effective date of the privacy policy.

(9) Whether any covered data collected by the covered entity or service provider is transferred to, processed in, retained in, or otherwise accessible to a foreign adversary (as determined by the Secretary of Commerce and specified in section 7.4 of title 15, Code of Federal Regulations (or any successor regulation)).

(c) LANGUAGES.—A privacy policy required under subsection (a) shall be made available to the public—

(1) in the 10 most-used languages in which a covered entity or service provider provides products or services or carries out activities related to such products or services; or

(2) if the covered entity or service provider provides products or services in fewer than 10 languages, in the languages in which the covered entity or service provider provides products or services or carries out activities related to such products or services.

(d) ACCESSIBILITY.—A covered entity or service provider shall provide the disclosures required under this section in a manner that is reasonably accessible to and usable by individuals living with disabilities.

(e) MATERIAL CHANGES.—

(1) NOTICE AND OPT OUT.—A covered entity that makes a material change to the privacy policy or practices of the covered entity shall—

(A) provide to each affected individual, in a clear and conspicuous manner—

(i) advance notice of such material change; and

(ii) a means to opt out of the collection, processing, retention, or transfer of any covered data of such individual pursuant to such material change; and

(B) with respect to the covered data of any individual who opts out using the means described in subparagraph (A)(ii), discontinue the collection, processing, retention, or transfer of such covered data, unless such collection, processing, retention, or transfer is necessary, proportionate, and limited to provide or maintain a product or service specifically requested by the individual.

(2) DIRECT NOTIFICATION.—A covered entity shall take all reasonable electronic measures to provide direct notification, if possible, to each affected individual regarding material changes to the privacy policy of the covered entity, and such notification shall be provided in each language in which the privacy policy is made available, taking into account available technology and the nature of the relationship between the covered entity and the individual.

(3) CLARIFICATION.—Except as provided in paragraph (1)(B), nothing in this subsection may be construed to affect the requirements for covered entities under sections 102, 105, and 106.

(f) TRANSPARENCY REQUIREMENTS FOR LARGE DATA HOLDERS.—

(1) RETENTION OF PRIVACY POLICIES; LOG OF MATERIAL CHANGES.—

(A) IN GENERAL.—Beginning on the date that is 180 days after the date of the enactment of this Act, each large data holder shall—

(i) retain and publish on the website of the large data holder a copy of each version of the privacy policy of the large data holder required under subsection (a) for not less than 10 years; and

(ii) make publicly available on the website of the large data holder, in a clear and conspicuous manner, a log that describes the date and nature of each material change to the privacy policy of the large data holder during the preceding 10-year period in a manner that is sufficient

for a reasonable individual to understand the effect of each material change.

(B) EXCLUSION.—This paragraph does not apply to material changes to previous versions of the privacy policy of a large data holder that precede the date that is 180 days after the date of the enactment of this Act.

(2) SHORT FORM NOTICE TO CONSUMERS.—

(A) IN GENERAL.—In addition to the privacy policy required under subsection (a), a large data holder shall provide a short-form notice of the covered data practices of the large data holder in a manner that—

(i) is concise;

(ii) is clear and conspicuous;

(iii) is readily accessible to an individual, based on the manner in which the individual interacts with the large data holder and the products or services of the large data holder and what is reasonably anticipated within the context of the relationship between the individual and the large data holder;

(iv) includes an overview of individual rights and disclosures to reasonably draw attention to data practices that may be unexpected or that involve sensitive covered data; and

(v) is not more than 500 words in length in the English language or, if in a language other than English, not more than 550 words in length.

(B) GUIDANCE.—Not later than 180 days after the date of the enactment of this Act, the Commission shall issue guidance establishing the minimum disclosures necessary for the short-form notice described in this paragraph and shall include templates or models for such notice.

SEC. 105. INDIVIDUAL CONTROL OVER COVERED DATA.

(a) ACCESS TO, AND CORRECTION, DELETION, AND PORTABILITY OF, COVERED DATA.—After receiving a verified request from an individual, including a parent acting on behalf of a child of the parent, a covered entity shall provide the individual with the right to—

(1) access—

(A) in a format that can be naturally read by a human, the covered data of the individual or child (as applicable) (or an accurate representation of the covered data of the individual or child (as applicable), if the covered data is no longer in the possession of the covered entity or a service provider acting

on behalf of the covered entity) that is collected, processed, or retained by the covered entity or any service provider of the covered entity;

(B) the name of any third party or service provider to whom the covered entity has transferred the covered data, as well as the categories of sources from which the covered data was collected; and

(C) a description of the purpose for which the covered entity transferred any covered data of the individual or child (as applicable) to a third party or service provider;

(2) correct any inaccuracy or incomplete information with respect to the covered data of the individual or child (as applicable) that is collected, processed, or retained by the covered entity and, for covered data that has been transferred, request the covered entity to notify any third party or service provider to which the covered entity transferred such covered data of the corrected information, including so that service providers may provide the assistance required by section 111(a)(1)(C);

(3) delete covered data of the individual or child (as applicable) that is retained by the covered entity and, for covered data that has been transferred, request that the covered entity notify any third party or service provider to which the covered entity transferred such covered data of the deletion request, including so that service providers may provide the assistance required by section 111(a)(1)(C);

(4) to the extent technically feasible, have exported covered data of the individual or child (as applicable) that is collected, processed, or retained by the covered entity, without licensing restrictions that unreasonably limit such transfers, in—

(A) a format that can be naturally read by a human; and

(B) a format that is portable, structured, interoperable, and machine-readable; and

(5) delete any content or information submitted to the covered entity by the individual when a covered minor and, for any such content or information that has been transferred, request that the covered entity notify any third party or service provider to which the covered entity transferred such content or information of the deletion request, including so that service providers may provide the assistance required by section 111(a)(1)(C).

(b) Frequency And Cost.—A covered entity—

(1) shall provide an individual with the opportunity to exercise each of the rights described in subsection (a); and

(2) with respect to—

(A) the first 3 instances that an individual exercises any right described in subsection (a) during any 12-month period, shall allow the individual to exercise such right free of charge; and

(B) any instance beyond the first 3 instances described in subparagraph (A), may charge a reasonable fee for each additional request to exercise any such right during such 12-month period.

(c) TIMING.—

(1) IN GENERAL.—Subject to subsections (b), (d), and (e), each request under subsection (a) shall be completed—

(A) by any covered entity that is a large data holder or data broker, not later than 30 calendar days after receiving such request from an individual, unless it is impossible or demonstrably impracticable to verify the individual; or

(B) by a covered entity that is not a large data holder or data broker, not later than 45 calendar days after receiving such request from an individual, unless it is impossible or demonstrably impracticable to verify the individual.

(2) EXTENSION.—A response period required under paragraph (1) may be extended once, by not more than the applicable time period described in such paragraph, when reasonably necessary, considering the complexity and number of requests from the individual, if the covered entity informs the individual of any such extension, and the reason for the extension, within the initial response period.

(d) VERIFICATION.—

(1) IN GENERAL.—A covered entity shall reasonably verify that an individual making a request to exercise a right described in subsection (a) is—

(A) the individual whose covered data is the subject of the request;

(B) the parent of the child whose covered data (or, with respect to a request under subsection (a)(5), whose content or other information) is the subject of the request; or

(C) another individual who is a natural person who is authorized to make such a request on behalf of the individual whose covered data is the subject of the request.

(2) ADDITIONAL INFORMATION.—If a covered entity cannot make the verification described in paragraph (1), the covered entity may request that the individual making the request provide any additional information necessary for the sole purpose of making such verification, except that—

(A) the request of the covered entity may not be burdensome on the individual; and

(B) the covered entity may not process, retain, or transfer such additional information for any other purpose.

(e) EXCEPTIONS.—

(1) REQUIRED EXCEPTIONS.—A covered entity may not permit an individual to exercise a right described in subsection (a), in whole or in part, if the covered entity—

(A) cannot reasonably make the verification described in subsection (d)(1);

(B) determines that exercise of the right would require access to, or the correction or deletion of, the sensitive covered data of an individual other than the individual whose covered data is the subject of the request;

(C) determines that exercise of the right would require correction or deletion of covered data subject to a warrant, lawfully executed subpoena, or litigation hold notice or equivalent preservation notice in connection with such warrant or subpoena or issued in a matter in which the covered entity is a named party;

(D) determines that exercise of the right would violate a Federal, State, Tribal, or local law that is not preempted by this title;

(E) determines that exercise of the right would violate the professional ethical obligations of the covered entity;

(F) reasonably believes that the request is made to further fraud;

(G) except with respect to health information, reasonably believes that the request is made in furtherance of criminal activity; or

(H) reasonably believes that complying with the request would threaten data security or network security.

(2) PERMISSIVE EXCEPTIONS.—A covered entity may decline, in whole or in part, to comply with a request to exercise a right described in subsection (a),

with adequate explanation to the individual making the request, if compliance with the request would—

(A) be demonstrably impracticable due to technological limitations or prohibitive cost, and if the covered entity provides a detailed description to the individual regarding the inability to comply with the request due to technological limitations or prohibitive cost;

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

(C) with respect to a right described in paragraph (1) or (4) of subsection (a), require the covered entity to release trade secrets or other privileged, proprietary, or confidential business information;

(D) prevent a covered entity from being able to maintain a confidential record of opt-out requests pursuant to this title that is maintained solely for the purpose of preventing covered data of an individual from being collected, processed, retained, or transferred after the individual submits an opt-out request;

(E) with respect to a deletion request, require a private elementary or secondary school (as determined under State law) or a private institution of higher education (as defined in title I of the Higher Education Act of 1965 (20 U.S.C. 1001 et seq.)) to delete covered data, if the deletion would unreasonably interfere with the provision of education services by, or the ordinary operation of, the school or institution;

(F) delete covered data that relates to a public figure regarding a matter of legitimate public interest and for which the requesting individual has no reasonable expectation of privacy; or

(G) delete covered data that the covered entity reasonably believes may be evidence of an abuse of the products or services of the covered entity, including a violation of terms of service.

(3) RULE OF CONSTRUCTION.—This section may not be construed to require a covered entity or service provider acting on behalf of a covered entity to —

(A) retain covered data collected for a 1-time transaction, if such covered data is not processed or transferred by the covered entity for any purpose other than completing such transaction;

(B) re-identify, or attempt to re-identify, de-identified data; or

(C) collect or retain any data in order to be capable of associating a request with the covered data that is the subject of the request.

(4) PARTIAL COMPLIANCE.—In the event a covered entity declines a request under paragraph (2), the covered entity shall comply with the remainder of the request if partial compliance is possible and not unduly burdensome.

(5) NUMBER OF REQUESTS.—For purposes of paragraph (2)(A), the receipt of a large number of verified requests, on its own, may not be considered to render compliance with a request demonstrably impracticable.

(6) ADDITIONAL EXCEPTIONS.—

(A) IN GENERAL.—The Commission may promulgate regulations, in accordance with section 553 of title 5, United States Code, to establish additional permissive exceptions to subsection (a) necessary to protect the rights of individuals, to alleviate undue burdens on covered entities, to prevent unjust or unreasonable outcomes from the exercise of access, correction, deletion, or portability rights, or to otherwise fulfill the purposes of this section.

(B) CONSIDERATIONS.—In establishing any exceptions under subparagraph (A), the Commission shall consider any relevant changes in technology, means for protecting privacy and other rights, and beneficial uses of covered data by covered entities.

(C) CLARIFICATION.—A covered entity may decline to comply with a request of an individual to exercise a right under this section pursuant to an exception the Commission establishes under this paragraph.

(f) LARGE DATA HOLDER METRICS REPORTING.—With respect to each calendar year for which an entity is a large data holder, such entity shall comply with the following requirements:

(1) REQUIRED METRICS.—Compile the following information for such calendar year:

(A) The number of verified access requests under subsection (a)(1).

(B) The number of verified deletion requests under subsection (a)(3).

(C) The number of verified deletion requests under subsection (a)(5).

(D) The number of verified requests to opt out of covered data transfers under section 106(a)(1).

(E) The number of verified requests to opt out of targeted advertising under section 106(a)(2).

(F) For each category of request described in subparagraphs (A) through (E), the number of such requests that the large data holder complied with in whole or in part.

(G) For each category of request described in subparagraphs (A) through (E), the average number of days within which the large data holder substantively responded to the requests.

(2) PUBLIC DISCLOSURE.—Not later than July 1 of each calendar year, disclose the information compiled under paragraph (1) for the previous calendar year—

(A) in the privacy policy of the large data holder; or

(B) on a publicly available website of the large data holder that is accessible from a hyperlink included in the privacy policy.

(g) GUIDANCE.—Not later than 1 year after the date of the enactment of this Act, the Commission shall issue guidance to clarify or explain the provisions of this section and establish practices by which a covered entity may verify a request to exercise a right described in subsection (a).

(h) ACCESSIBILITY.—

(1) LANGUAGE.—A covered entity shall facilitate the ability of individuals to make requests to exercise rights described in subsection (a) in any language in which the covered entity provides a product or service.

(2) INDIVIDUALS LIVING WITH DISABILITIES.—The mechanisms by which a covered entity enables individuals to make a request to exercise a right described in subsection (a) shall be readily accessible and usable by individuals living with disabilities.

SEC. 106. OPT-OUT RIGHTS AND UNIVERSAL MECHANISMS.

(a) IN GENERAL.—A covered entity shall provide to an individual the following opt-out rights with respect to the covered data of the individual:

(1) RIGHT TO OPT OUT OF COVERED DATA TRANSFERS TO THIRD PARTIES.—A covered entity—

(A) shall provide an individual with a clear and conspicuous means to opt out of the transfer of the covered data of the individual to a third party;

(B) upon establishment of an opt out mechanism that meets the requirements and technical specifications promulgated under subsection (b), shall allow an individual to make an opt-out designation pursuant to subparagraph (A) through the opt out mechanism;

(C) shall abide by an opt-out designation made pursuant to subparagraph (A) and communicate such designation to all relevant service providers and third parties; and

(D) except as provided in subsection (b) or (c)(4) of section 102, paragraph (3) or (4) of section 112(c), or section 120(b), need not allow an individual to opt out of a transfer of covered data made pursuant to a permissible purpose described in paragraph (1), (2), (3), (4), (5), (6), (7), (8), (9), (10), (11), (12), (13), or (14) of section 102(d).

(2) RIGHT TO OPT OUT OF TARGETED ADVERTISING.—A covered entity that engages in targeted advertising shall—

(A) provide an individual with a clear and conspicuous means to opt out of the processing and transfer of covered data of the individual in furtherance of targeted advertising;

(B) upon establishment of an opt out mechanism that meets the requirements and technical specifications promulgated under subsection (b), allow an individual to make an opt-out designation with respect to targeted advertising through the opt-out mechanism; and

(C) abide by any such opt-out designation made by an individual and communicate such designation to all relevant service providers and third parties.

(b) UNIVERSAL OPT-OUT MECHANISMS.—

(1) IN GENERAL.—Not later than 2 years after the date of the enactment of this Act, the Commission shall, in consultation with the Secretary of Commerce, promulgate regulations, in accordance with section 553 of title 5, United States Code, to establish requirements and technical specifications for 1 or more opt-out mechanisms (including global privacy signals, such as browser or device privacy settings) for individuals to exercise the opt-out rights established under this title through a single interface that—

(A) ensures that the opt-out preference signal—

(i) is clearly described, and easy-to-use by a reasonable individual;

(ii) does not require that an individual provide additional information beyond what is necessary to indicate such preference;

(iii) clearly represents the preference of an individual;

(iv) is provided—

(I) in the 10 most-used languages in which a covered entity provides products or services subject to the opt-out; or

(II) if the covered entity provides products or services subject to the opt-out in fewer than 10 languages, in the languages in which the covered entity provides such products or services; and

(v) is provided in a manner that is reasonably accessible to and usable by individuals living with disabilities;

(B) provides a mechanism for an individual to selectively opt out of the collection, processing, retention, or transfer of covered data by a covered entity, without affecting the preferences of the individual with respect to other entities or disabling the opt-out preference signal globally;

(C) states that, in the case of a page or setting view that the individual accesses to set the opt-out preference signal, the individual should see up to 2 choices, corresponding to the rights established under subsection (a); and

(D) ensures that the opt-out preference signal will be registered and set only by the individual or by another individual who is a natural person on behalf of the individual.

(2) EFFECT OF DESIGNATIONS.—A covered entity shall abide by any designation made by an individual through any mechanism that meets the requirements and technical specifications promulgated under paragraph (1).

SEC. 107. INTERFERENCE WITH CONSUMER RIGHTS.

(a) DARK PATTERNS PROHIBITED.—

(1) IN GENERAL.—A covered entity may not use dark patterns to—

(A) divert the attention of an individual from any notice required under this title;

(B) impair the ability of an individual to exercise any right under this title; or

(C) obtain, infer, or facilitate the consent of an individual for any action that requires the consent of an individual under this title.

(2) CLARIFICATION.—Any agreement by an individual that is obtained, inferred, or facilitated through dark patterns does not constitute consent for any purpose under this title.

(b) INDIVIDUAL AUTONOMY.—A covered entity may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of a right described in this title through the use of any false, fictitious, fraudulent, or materially misleading statement or representation.

SEC. 108. PROHIBITION ON DENIAL OF SERVICE AND WAIVER OF RIGHTS.

(a) RETALIATION THROUGH SERVICE OR PRICING PROHIBITED.—A covered entity may not retaliate against an individual for exercising any of the rights established under this title, or any regulations promulgated under this title, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services.

(b) RULES OF CONSTRUCTION.—

(1) BONA FIDE LOYALTY PROGRAMS.—

(A) IN GENERAL.—Nothing in subsection (a) may be construed to prohibit a covered entity from offering—

(i) to an individual different prices, rates, levels, qualities, or selections of goods or services, or functionalities with respect to a product or service, including offering goods or services for no fee, if the offering is in connection with the voluntary participation of the individual in a bona fide loyalty program, and if—

(I) the individual provided affirmative express consent to participate in such bona fide loyalty program;

(II) the covered entity abides by the exercise by the individual of any right provided by subsection (b) or (c) of section 102, section 105, or section 106; and

(III) the sale of covered data is not a condition of participation in the bona fide loyalty program; or

(ii) to an individual different prices, rates, levels, qualities, or selections of goods or services, or functionalities with respect to a product or service, based on the decision of the individual to terminate membership in a bona fide loyalty program or to exercise a right under

section 105(a)(3) to delete covered data that is necessary for participation in the bona fide loyalty program.

(B) BONA FIDE LOYALTY PROGRAM DEFINED.—For purposes of this section, the term "bona fide loyalty program"—

(i) includes rewards, premium features, discounts, and club card programs offered by a covered entity; and

(ii) excludes such programs offered by a covered high-impact social media company or data broker.

(2) MARKET RESEARCH.—Nothing in subsection (a) may be construed to prohibit a covered entity from offering a financial incentive or other consideration to an individual for participation in market research.

(3) DECLINING A PRODUCT OR SERVICE.—Nothing in subsection (a) may be construed to prohibit a covered entity from declining to provide a product or service or a bona fide loyalty program to an individual, if any collection, processing, retention, or transfer affected by the individual exercising a right established under this title is necessary, proportionate, and limited to providing such product or service.

SEC. 109. DATA SECURITY AND PROTECTION OF COVERED DATA.

(a) ESTABLISHMENT OF DATA SECURITY PRACTICES.—

(1) IN GENERAL.—Each covered entity or service provider shall establish, implement, and maintain reasonable data security practices to protect—

(A) the confidentiality, integrity, and availability of covered data; and

(B) covered data against unauthorized access.

(2) CONSIDERATIONS.—The data security practices required under paragraph (1) shall be appropriate to—

(A) the size and complexity of the covered entity or service provider;

(B) the nature and scope of the relevant collecting, processing, retaining, or transferring of covered data, taking into account changing business operations with respect to covered data;

(C) the volume, nature, and sensitivity of the covered data; and

(D) the state-of-the-art (and limitations thereof) in administrative, technical, and physical safeguards for protecting covered data.

(b) SPECIFIC REQUIREMENTS.—The data security practices required under subsection (a) shall include, at a minimum, the following:

(1) ASSESS VULNERABILITIES.—Routinely identifying and assessing any reasonably foreseeable internal or external risk to, or vulnerability in, each system maintained by the covered entity or service provider that collects, processes, retains, or transfers covered data, including unauthorized access to or corruption of such covered data, human vulnerabilities, access rights, and the use of service providers. Such activities shall include developing and implementing a plan for receiving and considering unsolicited reports of vulnerability by any entity and, if such a report is reasonably credible, performing a reasonable and timely investigation of such report and taking appropriate action to protect covered data against the vulnerability.

(2) PREVENTIVE AND CORRECTIVE ACTION.—

(A) IN GENERAL.—Taking preventive and corrective action to mitigate any reasonably foreseeable internal or external risk to, or vulnerability of, covered data identified by the covered entity or service provider, consistent with the nature of such risk or vulnerability and the role of the covered entity or service provider in collecting, processing, retaining, or transferring the data, which 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.

(B) EVALUATION OF PREVENTATIVE AND CORRECTIVE ACTION.—Evaluating and making reasonable adjustments to the action described in subparagraph (A) in light of any material changes in state-of-the-art technology, internal or external threats to covered data, and changing business operations with respect to covered data.

(3) INFORMATION RETENTION AND DISPOSAL.—Disposing of covered data (either by or at the direction of the covered entity) that is required to be deleted by law or is no longer necessary for the purpose for which the data was collected, processed, retained, or transferred, unless a permitted purpose under section 102(d) applies, except that retention and disposal of biometric information shall be governed by section 102(c)(3). 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 section.

(4) RETENTION SCHEDULE.—Developing, maintaining, and adhering to a retention schedule for covered data consistent with paragraph (3).

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

(6) INCIDENT RESPONSE.—Implementing procedures to detect, respond to, and recover from data security incidents, including breaches.

(c) REGULATIONS.—The Commission may, in consultation with the Secretary of Commerce, promulgate, in accordance with section 553 of title 5, United States Code, technology-neutral, process-based regulations to carry out this section.

SEC. 110. EXECUTIVE RESPONSIBILITY.

(a) DESIGNATION OF PRIVACY AND DATA SECURITY OFFICERS.—

(1) IN GENERAL.—A covered entity or service provider (except for a large data holder) shall designate 1 or more qualified employees to serve as privacy and data security officers.

(2) REQUIREMENTS FOR OFFICERS.—An employee who is designated by a covered entity or service provider as a privacy and data security officer shall, at a minimum—

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

(B) facilitate the ongoing compliance of the covered entity or service provider with this title.

(b) REQUIREMENTS FOR LARGE DATA HOLDERS.—

(1) DESIGNATION.—A covered entity or service provider that is a large data holder shall designate 1 qualified employee to serve as a privacy officer and 1 qualified employee to serve as a data security officer.

(2) ANNUAL CERTIFICATION.—

(A) IN GENERAL.—Beginning on the date that is 1 year after the date of the enactment of this Act, the chief executive officer of a large data holder (or, if the large data holder does not have a chief executive officer, the highest ranking officer of the large data holder) and each privacy officer and data security officer of such large data holder designated under paragraph (1), shall annually certify to the Commission, in a manner specified by the Commission, that the large data holder implements and maintains—

(i) internal controls reasonably designed, implemented, maintained, and monitored to comply with this title; and

(ii) internal reporting structures (as described in paragraph (3)) to ensure that such certifying officers are involved in, and responsible for, decisions that impact compliance by the large data holder with this title.

(B) REQUIREMENTS.—A certification submitted under subparagraph (A) 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 officers not more than 90 days before the submission of the certification.

(3) INTERNAL REPORTING STRUCTURE REQUIREMENTS.—At least 1 of the officers designated under paragraph (1) shall, either directly or through a supervised designee—

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

(B) conduct biennial and comprehensive audits to ensure the policies, practices, and procedures of the large data holder comply with this title and, upon request, make such audits available to the Commission;

(C) develop a program to educate and train employees about the requirements of this title;

(D) maintain updated, accurate, clear, and understandable records of all significant privacy and data security practices of the large data holder; and

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

(4) PRIVACY IMPACT ASSESSMENTS.—

(A) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act or 1 year after the date on which an entity first meets the definition of the term "large data holder", whichever is earlier, and biennially thereafter, each large data holder shall conduct a privacy impact assessment that weighs the benefits of the covered data collection, processing, retention, and transfer practices of the entity against the potential 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 and volume of the covered data collected, processed, retained, or transferred by the large data holder; and

(II) the potential risks posed to the privacy of individuals by the collection, processing, retention, and transfer of covered data by the large data holder;

(ii) documented in written form and maintained by the large data holder for as long as the relevant privacy policy is required to be retained under section 104(f)(1); and

(iii) approved by the privacy officer of the large data holder.

(C) ADDITIONAL FACTORS TO INCLUDE IN ASSESSMENT.—In assessing privacy risks for purposes of an assessment conducted under subparagraph (A), including significant risks of harm to the privacy of an individual or the security of covered data, the large data holder shall include reviews of the means by which technologies, including blockchain and distributed ledger technologies and other emerging technologies, including privacy enhancing technologies, are used to secure covered data.

SEC. 111. SERVICE PROVIDERS AND THIRD PARTIES.

(a) SERVICE PROVIDERS.—

(1) IN GENERAL.—A service provider that collects, processes, retains, or transfers covered data on behalf of or at the direction of a covered entity or another service provider—

(A) shall adhere to the instructions of the covered entity or other service provider and collect, process, retain, or transfer covered data only to the extent necessary, proportionate, and limited to provide a service requested by the covered entity or other service provider, as set out in the contract described in paragraph (2);

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

(C) shall assist the covered entity or other service provider in fulfilling the obligations of the covered entity or other service provider to respond to consumer rights requests pursuant to this title by—

(i) providing appropriate technical and organizational support, taking into account the nature of the processing and the information reasonably available to the service provider; or

(ii) fulfilling a request by the covered entity or other service provider to execute a consumer rights request that the covered entity or other service provider has determined should be compiled with, by either—

(I) complying with the request pursuant to the instructions of the covered entity or other service provider; or

(II) providing written verification to the covered entity or other service provider that the service provider does not hold data related to the request, that complying with the request would be inconsistent with the legal obligations of the service provider, or that the request falls within an exception pursuant to this title;

(D) shall, upon the reasonable request of the covered entity or other service provider, make available to the covered entity or other service provider all information necessary to demonstrate the compliance of the service provider with the requirements of this title;

(E) shall delete or return, as directed by the covered entity or other service provider, all covered data as soon as practicable after the contractually agreed upon end of the provision of services, unless the retention by the service provider of covered data is required by law;

(F) may engage another service provider for purposes of processing or retaining covered data on behalf of the covered entity or other service provider only after exercising reasonable care in selecting another service provider as required by subsection (d), providing the covered entity or other service provider with written notice of the engagement, and entering into a written contract that requires the other service provider to satisfy the requirements of this title with respect to covered data; and

(G) shall—

(i) allow and cooperate with reasonable assessments by the covered entity or other service provider at least annually; or

(ii) arrange for a qualified and independent assessor to conduct an assessment of the policies and technical and organizational measures of the service provider in support of the obligations of the service provider under this title at least annually, using an appropriate and accepted control standard or framework and assessment procedure for such assessments, and report the results of such assessment to the covered entity or other service provider.

(2) CONTRACT REQUIREMENTS.—An entity may only operate as a service provider pursuant to a contract between a covered entity and a service provider. Such contract—

(A) shall govern the data processing procedures of the service provider with respect to any collection, processing, retention, or transfer performed on behalf of the covered entity;

(B) shall clearly set forth—

(i) instructions for collecting, processing, retaining, or transferring data;

(ii) the nature and purpose of the collection, processing, retention, or transfer;

(iii) the type of data subject to collection, processing, retention, or transfer;

(iv) the duration of the processing or retention; and

(v) the rights and obligations of both parties;

(C) may not relieve the covered entity or service provider of any obligation under this title; and

(D) shall prohibit—

(i) the collection, processing, retention, or transfer of covered data in a manner that does not comply with the requirements of paragraph (1); and

(ii) combining covered data that the service provider receives from or on behalf of a covered entity with covered data that the service provider receives from or on behalf of another entity or collects from the interaction of the service provider with an individual, unless such combining is necessary for a purpose described in section 102(d), other than a purpose described in paragraph (7), (14), (15), or (16) of such section, and is otherwise permitted under the contract.

(b) THIRD PARTIES.—

(1) IN GENERAL.—A third party may not process, retain, or transfer third-party data for a purpose other than—

(A) in the case of sensitive covered data—

(i) except as provided in clause (ii), a purpose for which an individual gave affirmative express consent pursuant to subsection (b) or (c) of section 102; or

(ii) in the case of sensitive covered data with respect to which affirmative express consent is not required pursuant to subsection (b) of section 102, a purpose for which the covered entity or service provider made a disclosure pursuant to section 104; or

(B) in the case of covered data that is not sensitive covered data, a purpose for which the covered entity or service provider made a disclosure pursuant to section 104.

(2) CONTRACT REQUIREMENTS.—Before transferring covered data to a third party, a covered entity or service provider shall enter into a contract with the third party that—

(A) identifies the purposes for which covered data is being transferred;

(B) specifies that the third party may only use the covered data for such purposes;

(C) with respect to the covered data transferred, requires the third party to comply with all applicable provisions of, and regulations promulgated under, this title;

(D) requires the third party to notify the covered entity or service provider if the third party makes a determination that the third party can no longer meet the obligations of the third party under this title; and

(E) grants the covered entity or service provider the right, upon notice (including under subparagraph (D)), to take reasonable and appropriate steps to stop and remediate unauthorized use of covered data by the third party.

(c) RULES OF CONSTRUCTION.—

(1) SUCCESSIVE ACTOR VIOLATIONS.—

(A) IN GENERAL.—With respect to a violation of this title by a service provider or third party regarding covered data received by the service provider or third party from a covered entity or another service provider, the covered entity or service provider that transferred such covered data may not be considered to be in violation of this title if the covered entity or service provider transferred the covered data in compliance with the requirements of this title and, at the time of transferring such covered data, did not have actual knowledge, or reason to believe, that the service provider or third party to which the covered data was transferred intended to violate this title.

(B) KNOWLEDGE OF VIOLATION.—A covered entity or service provider that transfers covered data to a service provider or third party and has actual knowledge, or reason to believe, that such service provider or third party is violating, or is about to violate, the requirements of this title shall immediately cease the transfer of covered data to such service provider or third party.

(2) PRIOR ACTOR VIOLATIONS.—An entity that collects, processes, retains, or transfers covered data in compliance with the requirements of this title may not be considered to be in violation of this title as a result of a violation by an entity from which it receives, or on whose behalf it collects, processes, retains, or transfers, covered data.

(d) REASONABLE CARE.—

(1) SERVICE PROVIDER SELECTION.—A covered entity or service provider shall exercise reasonable care in selecting a service provider.

(2) TRANSFER TO THIRD PARTY.—A covered entity or service provider shall exercise reasonable care in deciding to transfer covered data to a third party.

(3) GUIDANCE.—Not later than 2 years after the date of the enactment of this Act, the Commission shall publish guidance regarding compliance with this subsection.

(e) RULE OF CONSTRUCTION.—Solely for purposes of this section, the requirements under this section for service providers to contract with, assist, and follow the instructions of covered entities shall also apply to any entity that collects, processes, retains, or transfers covered data for the purpose of performing services on behalf of, or at the direction of, a government entity, as though such government entity were a covered entity.

SEC. 112. DATA BROKERS.

(a) NOTICE.—A data broker shall—

(1) establish and maintain a publicly available website; and

(2) place a clear and conspicuous, and not misleading, notice on such publicly available website, and any mobile application of the data broker, that—

(A) states that the entity is a data broker;

(B) states that an individual may exercise a right described in section 105 or 106, and includes a link or other tool to allow an individual to exercise such right;

(C) includes a link to the website described in subsection (c)(3);

(D) is reasonably accessible to and usable by individuals living with disabilities; and

(E) is provided in any language in which the data broker provides products or services.

(b) PROHIBITED PRACTICES.—A data broker may not—

(1) advertise or market access to, or the transfer of, covered data for the purposes of—

(A) stalking or harassing an individual; or

(B) engaging in fraud, identity theft, or unfair or deceptive acts or practices; or

(2) misrepresent the business practices of the data broker.

(c) DATA BROKER REGISTRATION.—

(1) IN GENERAL.—Not later than January 31 of each calendar year that follows a calendar year during which an entity acted as a data broker with respect to more than 5,000 individuals or devices that identify or are linked or reasonably linkable to an individual, such entity shall register with the Commission in accordance with this subsection.

(2) REGISTRATION REQUIREMENTS.—In registering with the Commission as required under paragraph (1), a data broker shall do the following:

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

(B) Provide the Commission with the following information:

(i) The legal name and primary valid physical postal address, email address, and internet address of the data broker.

(ii) A description of the categories of covered data the data broker collects, processes, retains, or transfers.

(iii) The contact information of the data broker, including the name of a contact person, a human-monitored telephone number, a human-monitored e-mail address, a website, and a physical mailing address.

(iv) A link to a website through which an individual may easily exercise the rights described in sections 105 and 106.

(3) DATA BROKER REGISTRY.—

(A) ESTABLISHMENT.—The Commission shall establish and maintain on a publicly available website a searchable list of data brokers that are registered with the Commission under this subsection.

(B) REQUIREMENTS.—The registry established under subparagraph (A) shall—

(i) allow members of the public to search for and identify data brokers;

(ii) include the information required under paragraph (2)(B) for each data broker;

(iii) include a mechanism by which an individual, including a parent acting on behalf of a child of the parent, may submit to all registered data brokers a "Do Not Collect" request that results in registered data brokers no longer collecting covered data related to such individual or child (as applicable) without the affirmative express consent of such individual; and

(iv) include a mechanism by which an individual, including a parent acting on behalf of a child of the parent, may submit to all registered data brokers a "Delete My Data" request that results in registered data brokers deleting all covered data related to such individual or child (as applicable) that the data broker did not collect directly from such individual or when acting as a service provider.

(C) AFFORDABILITY.—A data broker may not charge an individual a fee to exercise a right under this paragraph.

(4) DO NOT COLLECT AND DELETE MY DATA REQUESTS.—

(A) COMPLIANCE.—Subject to subparagraph (B), each data broker that receives a request from an individual, including a parent acting on behalf of a child of the parent, using the mechanism established under paragraph (3)(B)(iii) or paragraph (3)(B)(iv) shall comply with such request not later than 30 days after the date on which the request is received by the data broker.

(B) EXCEPTION.—A data broker may decline to fulfill a request from an individual, if—

(i) the data broker has actual knowledge that the individual has been convicted of a crime related to the abduction or sexual exploitation of a child; and

(ii) the data collected by the data broker is necessary—

(I) to carry out a national or State-run sex offender registry; or

(II) for the National Center for Missing and Exploited Children.

SEC. 113. COMMISSION-APPROVED COMPLIANCE GUIDELINES.

(a) APPLICATION FOR COMPLIANCE GUIDELINE APPROVAL.—

(1) IN GENERAL.—A covered entity that is not a data broker and is not a large data holder, 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, retention, or transfer of covered data by the covered entity or covered entities.

(2) APPLICATION REQUIREMENTS.—An application under paragraph (1) shall include—

(A) a description of how the proposed guidelines will meet or exceed the applicable requirements of this title;

(B) a description of the entities or activities the proposed guidelines are designed to cover;

(C) a list of the covered entities, to the extent known at the time of application, that intend to adhere to the proposed guidelines;

(D) a description of an independent organization, not associated with any of the intended adhering covered entities, that will administer the proposed guidelines; and

(E) a description of how such intended adhering entities will be assessed for adherence to the proposed guidelines by the independent organization described in subparagraph (D).

(3) COMMISSION REVIEW.—

(A) INITIAL APPROVAL.—

(i) PUBLIC COMMENT PERIOD.—Not later than 90 days after receipt of an application regarding proposed guidelines submitted pursuant to paragraph (1), the Commission shall publish the application

and provide an opportunity for public comment on such proposed guidelines.

(ii) APPROVAL CRITERIA.—The Commission shall approve an application regarding proposed guidelines submitted pursuant to paragraph (1), including the independent organization that will administer the guidelines, if the applicant demonstrates that the proposed guidelines—

(I) meet or exceed the applicable requirements of this title;

(II) provide for regular review and validation by an independent organization to ensure that the covered entity or covered entities adhering to the guidelines continue to meet or exceed the applicable requirements of this title; 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 under section 115 or referral to the appropriate State attorney general for enforcement under section 116.

(iii) TIMELINE.—Not later than 1 year after the date on which the Commission receives an application regarding proposed guidelines pursuant to paragraph (1), the Commission shall issue a determination approving or denying the application, including the relevant independent organization, and providing the reasons for approving or denying the application.

(B) APPROVAL OF MODIFICATIONS.—

(i) IN GENERAL.—If the independent organization administering a set of guidelines approved under subparagraph (A) makes significant changes to the guidelines, 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 significant change to guidelines submitted under clause (i) not later than 180 days after the date on which the Commission receives the submission for approval.

(b) WITHDRAWAL OF APPROVAL.—

(1) IN GENERAL.—If at any time the Commission determines that guidelines previously approved under this section no longer meet the applicable requirements of this title or that compliance with the approved guidelines is insufficiently enforced by the independent organization administering the guidelines, the Commission shall notify the relevant covered entity or group of covered entities and the independent organization of the determination of the Commission to withdraw approval of the guidelines, including the basis for the determination.

(2) OPPORTUNITY TO CURE.—

(A) IN GENERAL.—Not later than 180 days after receipt of a notice under paragraph (1), the covered entity or group of covered entities and the independent organization may cure any alleged deficiency with the guidelines or the enforcement of the guidelines and submit each proposed cure to the Commission.

(B) EFFECT ON WITHDRAWAL OF APPROVAL.—If the Commission determines that cures proposed under subparagraph (A) eliminate alleged deficiencies in the guidelines, the Commission may not withdraw the approval of such guidelines on the basis of such deficiencies.

(c) CERTIFICATION.—A covered entity with guidelines approved by the Commission under this section shall—

(1) publicly self-certify that the covered entity is in compliance with the guidelines; and

(2) as part of the self-certification under paragraph (1), indicate the independent organization responsible for assessing compliance with the guidelines.

(d) REBUTTABLE PRESUMPTION OF COMPLIANCE.—A covered entity that is eligible to participate in guidelines approved under this section, participates in the guidelines, and is in compliance with the guidelines shall be entitled to a rebuttable presumption that the covered entity is in compliance with the relevant provisions of this title to which the guidelines apply.

(e) ELIGIBILITY OF SERVICE PROVIDERS.—This section shall apply to a service provider that is not a large data holder, or a group of such service providers, in the same manner as this section applies to a covered entity or group of covered entities. Such a service provider or group of service providers may apply for approval of, and participate in, the same guidelines as a covered entity or group of covered entities.

SEC. 114. PRIVACY-ENHANCING TECHNOLOGY PILOT PROGRAM.

(a) PRIVACY-ENHANCING TECHNOLOGY DEFINED.—In this section, the term "privacy-enhancing technology"—

(1) means any software or hardware solution, cryptographic algorithm, or other technical process of extracting the value of information without substantially reducing the privacy and security of the information; and

(2) includes technologies with functionality similar to homomorphic encryption, differential privacy, zero-knowledge proofs, synthetic data generation, federated learning, and secure multi-party computation.

(b) ESTABLISHMENT.—Not later than 1 year after the date of the enactment of this Act, the Commission shall establish and carry out a pilot program to encourage private sector use of privacy-enhancing technologies for the purposes of protecting covered data to comply with section 109.

(c) PURPOSES.—Under the pilot program established under subsection (b), the Commission shall—

(1) develop and implement a petition process for covered entities to request to be a part of the pilot program; and

(2) build an auditing system that leverages privacy-enhancing technologies to support the enforcement actions of the Commission.

(d) PETITION PROCESS.—A covered entity wishing to be accepted into the pilot program established under subsection (b) shall demonstrate to the Commission that the privacy-enhancing technologies to be used under the pilot program by the covered entity will establish data security practices that meet or exceed all or some of the requirements in section 109. If the covered entity demonstrates the privacy-enhancing technologies meet or exceed the requirements in section 109, the Commission may accept the covered entity to be a part of the pilot program. If the Commission does not accept a covered entity to be a part of the pilot program, the Commission shall provide an adequate response to the covered entity detailing why the covered entity was not accepted, and the covered entity may subsequently revise the petition of the covered entity to address any deficiencies indicated by the Commission in the response of the Commission to the covered entity.

(e) REQUIREMENTS.—In carrying out the pilot program established under subsection (b), the Commission shall—

(1) receive input from private, public, and academic stakeholders; and

(2) develop ongoing public and private sector engagement, in consultation with the Secretary of Commerce, to disseminate voluntary, consensus-based resources to increase the integration of privacy-enhancing technologies in data collection, sharing, and analytics by the public and private sectors.

(f) CONCLUSION OF PILOT PROGRAM.—The Commission shall terminate the pilot program established under subsection (b) not later than 10 years after the

commencement of the program.

(g) STUDY REQUIRED.—

(1) IN GENERAL.—The Comptroller General of the United States shall conduct a study—

(A) to assess the progress of the pilot program established under subsection (b);

(B) to determine the effectiveness of using privacy-enhancing technologies at the Commission to support oversight of the data security practices of covered entities; and

(C) to develop recommendations to improve and advance privacy-enhancing technologies, including by improving communication and coordination between covered entities and the Commission to increase implementation of privacy-enhancing technologies by such entities and the Commission.

(2) INITIAL BRIEFING.—Not later than 3 years after the date of the enactment of this Act, the Comptroller General shall brief the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on the initial results of the study conducted under paragraph (1).

(3) FINAL REPORT.—Not later than 240 days after the date on which the briefing required by paragraph (2) is conducted, the Comptroller General shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a final report setting forth the results of the study conducted under paragraph (1), including the recommendations developed under subparagraph (C) of such paragraph.

(h) AUDIT OF COVERED ENTITIES.—The Commission shall, on an ongoing basis, audit covered entities who have been accepted to be part of the pilot program established under subsection (b) to determine whether such a covered entity is maintaining the use and implementation of privacy-enhancing technologies to secure covered data.

(i) WITHDRAWAL FROM THE PILOT PROGRAM.—If at any time the Commission determines that a covered entity accepted to be a part of the pilot program established under subsection (b) is no longer maintaining the use of privacy-enhancing technologies, the Commission shall notify the covered entity of the determination of the Commission to withdraw approval for the covered entity to be a part of the pilot program and the basis for doing so. Not later than 180 days after the date on which a covered entity receives such notice, the covered entity may cure any alleged deficiency

with the use of privacy-enhancing technologies and submit each proposed cure to the Commission. If the Commission determines that such cures eliminate alleged deficiencies with the use of privacy-enhancing technologies, the Commission may not withdraw the approval of the covered entity to be a part of the pilot program on the basis of such deficiencies.

(j) LIMITATIONS ON LIABILITY.—Any covered entity that petitions, and is accepted, to be part of the pilot program established under subsection (b), actively implements and maintains the use of privacy-enhancing technologies, and is determined by the Commission to be in compliance with the program shall—

(1) for any action under section 115 or 116 for a violation of section 109, be deemed to be in compliance with section 109 with respect to the covered data subject to the privacy-enhancing technologies; and

(2) for any action under section 117 for a violation of section 109, be entitled to a rebuttable presumption that such entity is in compliance with section 109 with respect to the covered data subject to the privacy-enhancing technologies.

SEC. 115. ENFORCEMENT BY FEDERAL TRADE COMMISSION.

(a) NEW BUREAU.—

(1) IN GENERAL.—Subject to the availability of appropriations, the Commission shall establish, within the Commission, a new bureau comparable in structure, size, organization, and authority to the existing bureaus within the Commission related to consumer protection and competition.

(2) MISSION.—The mission of the bureau established under this subsection shall be to assist the Commission in exercising the authority of the Commission under this title and related authorities.

(3) STAFF.—

(A) IN GENERAL.—In staffing the bureau established under this subsection, the Commission shall ensure the allocation of full time employees or full time employee equivalents that include attorneys, economists, investigators, technologists, and mental health professionals with experience in the well-being of children and teens.

(B) TECHNOLOGIST DEFINED.—For the purposes of this paragraph, the term "technologist" means an individual with training and expertise with respect to technology, including state-of-the art information technology, network or data security, hardware or software development, privacy-enhancing technologies, cryptography, computer science, data science, advertising technology, web tracking, machine learning, and other related fields and applications.

(4) TIMELINE.—The bureau established under this subsection shall be established, staffed, and fully operational not later than 180 days after the date of the enactment of this Act.

(b) ENFORCEMENT BY COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this title or a regulation promulgated under this title shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) POWERS OF COMMISSION.—

(A) IN GENERAL.—Except as provided in paragraph (3) or otherwise provided in this title, the Commission shall enforce this title and the regulations promulgated under this title 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 title.

(B) PRIVILEGES AND IMMUNITIES.—Any entity that violates this title or a regulation promulgated under this title shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(3) COMMON CARRIERS AND NONPROFITS.—Notwithstanding section 4, 5(a)(2), or 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 title, and the regulations promulgated under this title, in the same manner provided in paragraphs (1) and (2) of this subsection with respect to—

(A) common carriers subject to title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.); and

(B) organizations not organized to carry on business for their own profit or that of their members.

(4) PENALTY OFFSET FOR STATE OR INDIVIDUAL ACTIONS.—Any amount that a court orders an entity to pay in an action brought under this subsection shall be offset by any amount a court has ordered the entity to pay in an action brought against the entity for the same violation under section 116 or 117.

(5) PRIVACY AND SECURITY VICTIMS RELIEF FUND.—

(A) ESTABLISHMENT OF VICTIMS RELIEF FUND.—There is established in the Treasury of the United States a separate fund to be known as the "Privacy and Security Victims Relief Fund" (in this paragraph referred to as the "Victims Relief Fund").

(B) DEPOSITS.—The Commission or the Attorney General of the United States, as applicable, shall deposit into the Victims Relief Fund the amount of any civil penalty obtained in any civil action the Commission, or the Attorney General on behalf of the Commission, commences to enforce this title or a regulation promulgated under this title.

(C) USE OF FUND AMOUNTS.—

(i) AVAILABILITY TO THE COMMISSION.—Notwithstanding section 3302 of title 31, United States Code, amounts in the Victims Relief Fund shall be available to the Commission, without fiscal year limitation, to provide redress, damages, payments or compensation, or other monetary relief to persons affected by an act or practice for which civil penalties, other monetary relief, or any other forms of relief (including injunctive relief) have been ordered in a civil action or administrative proceeding the Commission commences, or in any civil action the Attorney General of the United States commences on behalf of the Commission, to enforce this title or a regulation promulgated under this title.

(ii) OTHER PERMISSIBLE USES.—To the extent that individuals cannot be located or such redress, damages, payments or compensation, or other monetary relief are otherwise not practicable, the Commission may use amounts in the Victims Relief Fund for the purpose of—

(I) consumer or business education relating to data privacy or data security; or

(II) engaging in technological research that the Commission considers necessary to implement this title, including promoting privacy-enhancing technologies that promote compliance with this title.

(D) CALCULATION.—Any amount that the Commission provides to a person as redress, payments or compensation, or other monetary relief under subparagraph (C) with respect to a violation by an entity shall be offset by any amount the person received from an action brought against the entity for the same violation under section 116 or 117.

(E) RULE OF CONSTRUCTION.—Amounts collected and deposited in the Victims Relief Fund may not be construed to be Government funds or

appropriated monies and may not be subject to apportionment for the purpose of chapter 15 of title 31, United States Code, or under any other authority.

(c) REPORT.—

(1) IN GENERAL.—Not later than 4 years after the date of the enactment of this Act, and annually thereafter, the Commission shall submit to Congress a report describing investigations conducted during the prior year with respect to violations of this title, including—

(A) the number of such investigations the Commission commenced;

(B) the number of such investigations the Commission closed with no official agency action;

(C) the disposition of such investigations, if such investigations have concluded and resulted in official agency action; and

(D) for each investigation that was closed with no official agency action, the industry sectors of the covered entities subject to each investigation.

(2) PRIVACY PROTECTIONS.—A report required under paragraph (1) may not include the identity of any person who is the subject of an investigation or any other information that identifies such a person.

(3) ANNUAL PLAN.—Not later than 540 days after the date of the enactment of this Act, and annually thereafter, the Commission shall submit to Congress a plan for the next calendar year describing the projected activities of the Commission under this title, including—

(A) the policy priorities of the Commission and any changes to the previous policy priorities of the Commission;

(B) any rulemaking proceedings projected to be commenced, including any such proceedings to amend or repeal a rule;

(C) any plans to develop, update, or withdraw guidelines or guidance required under this title;

(D) any plans to restructure the Commission; and

(E) projected dates and timelines, or changes to projected dates and timelines, associated with any of the requirements under this title.

SEC. 116. ENFORCEMENT BY STATES.

(a) CIVIL ACTION.—

(1) IN GENERAL.—In any case in which the attorney general of a State, the chief consumer protection officer of a State, or an officer or office of a State authorized to enforce privacy or data security laws applicable to covered entities or service providers has reason to believe that an interest of the residents of the State has been or is adversely affected by the engagement of any entity in an act or practice that violates this title or a regulation promulgated under this title, the attorney general, chief consumer protection officer, or other authorized officer or office of the State may bring a civil action in the name of the State, or as parens patriae on behalf of the residents of the State, in an appropriate Federal district court of the United States to—

(A) enjoin such act or practice;

(B) enforce compliance with this title or the regulations promulgated under this title;

(C) obtain civil penalties;

(D) obtain damages, restitution, or other compensation on behalf of the residents of the State;

(E) obtain reasonable attorney's fees and other litigation costs reasonably incurred; or

(F) obtain such other relief as the court may consider to be appropriate.

(2) LIMITATION.—In any case with respect to which the attorney general of a State, the chief consumer protection officer of a State, or an officer or office of a State authorized to enforce privacy or data security laws applicable to covered entities or service providers brings an action under paragraph (1), no other officer or office of the same State may institute a civil action under paragraph (1) against the same defendant for the same violation of this title or regulation promulgated under this title.

(b) RIGHTS OF THE COMMISSION.—

(1) IN GENERAL.—Except if not feasible, a State officer shall notify the Commission in writing prior to initiating a civil action under subsection (a). Such notice shall include a copy of the complaint to be filed to initiate such action. Upon receiving such notice, the Commission may intervene in such action and, upon intervening—

(A) be heard on all matters arising in such action; and

(B) file petitions for appeal of a decision in such action.

(2) NOTIFICATION TIMELINE.—If not feasible for a State officer to provide the notification required by paragraph (1) before initiating a civil action under subsection (a), the State officer shall notify the Commission immediately after initiating the civil action.

(c) ACTIONS BY THE COMMISSION.—In any case in which a civil action is instituted by or on behalf of the Commission for a violation of this title or a regulation promulgated under this title, no attorney general of a State, chief consumer protection officer of a State, or officer or office of a State authorized to enforce privacy or data security laws may, during the pendency of such action, institute a civil action against any defendant named in the complaint in the action instituted by or on behalf of the Commission for a violation of this title or a regulation promulgated under this title that is alleged in such complaint.

(d) INVESTIGATORY POWERS.—Nothing in this title may be construed to prevent the attorney general of a State, the chief consumer protection officer of a State, or an officer or office of a State authorized to enforce privacy or data security laws applicable to covered entities or service providers from exercising the powers conferred on such officer or office to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in any Federal district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(2) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

(f) GAO STUDY.—

(1) IN GENERAL.—The Comptroller General of the United States shall conduct a study of the practice of State attorneys general hiring, or otherwise contracting with, outside firms to assist in enforcement efforts pursuant to this title, which shall include the study of—

(A) the frequency with which each State attorney general hires or contracts with outside firms to assist in such enforcement efforts;

(B) the contingency fees, hourly rates, and other costs of hiring or contracting with outside firms;

(C) the types of matters for which outside firms are hired or contracted;

(D) the bid and selection process for such outside firms, including reviews of conflicts of interest;

(E) the practices State attorneys general set in place to protect sensitive information that would become accessible by outside firms while the outside firms are assisting in such enforcement efforts;

(F) the percentage of monetary recovery that is returned to victims and the percentage of such recovery that is retained by outside firms; and

(G) the market average for the hourly rate of hired or contracted attorneys in each market.

(2) REPORT.—Not later than 1 year after the date of the enactment of this Act, the Comptroller General shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on the results of the study conducted under paragraph (1).

(g) PRESERVATION OF STATE POWERS.—Except as provided in subsections (a)(2) and (c), no provision of this section may be construed as altering, limiting, or affecting the authority of a State attorney general, the chief consumer protection officer of a State, or an officer or office of a State authorized to enforce laws applicable to covered entities or service providers to—

(1) bring an action or other regulatory proceeding arising solely under the laws in effect in such State; or

(2) exercise the powers conferred on the attorney general, chief consumer protection officer, or officer or office by the laws of such State, including the ability to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

(h) CALCULATION.—Any amount that a court orders an entity to pay to a person under this section shall be offset by any amount the person received from an action brought against the entity for the same violation under section 115 or 117.

SEC. 117. ENFORCEMENT BY PERSONS.

(a) CIVIL ACTION.—

(1) IN GENERAL.—Subject to subsections (b) and (c), a person may bring a civil action against a covered entity or service provider for a violation of subsection (b) or (c) of section 102, subsection (a) or (e) of section 104, section 105, subsection (a) or (b)(2) of section 106, section 107, section 108, section 109 to the extent such action alleges a data breach arising from a violation of subsection (a) of such section, subsection (d) of section 111, or subsection (c)(4) of section 112, or a regulation promulgated thereunder, in an appropriate Federal district court of the United States.

(2) RELIEF.—

(A) IN GENERAL.—In a civil action brought under paragraph (1) in which the plaintiff prevails, the court may award the plaintiff—

(i) an amount equal to the sum of any actual damages;

(ii) injunctive relief, including an order that an entity retrieve any covered data transferred in violation of this title;

(iii) declaratory relief; and

(iv) reasonable attorney fees and litigation costs.

(B) BIOMETRIC AND GENETIC INFORMATION.—In a civil action brought under paragraph (1) for a violation of this title with respect to section 102(c), in which the plaintiff prevails, if the conduct underlying the violation occurred primarily and substantially in Illinois, the court may award the plaintiff—

(i) for a violation involving biometric information, the same relief as set forth in section 20 of the Biometric Information Privacy Act (740 ILCS 14/20), as such statute reads on December 31, 2024; or

(ii) for a violation involving genetic information, the same relief as set forth in section 40 of the Genetic Information Privacy Act (410 ILCS 513/40), as such statute reads on December 31, 2024.

(C) DATA SECURITY.—

(i) IN GENERAL.—In a civil action brought under paragraph (1) for a violation of this title alleging unauthorized access of covered information as a result of a violation of section 109(a), in which the plaintiff prevails, the court may award a plaintiff who is a resident of California the same relief as set forth in section 1798.150 of the California Civil Code, as such statute read on January 1, 2024.

(ii) COVERED INFORMATION DEFINED.—For purposes of this subparagraph, the term "covered information" means the following:

(I) A username, email address, or telephone number of an individual in combination with a password or security question or answer that would permit access to an account held by the individual that contains or provides access to sensitive covered data.

(II) The first name or first initial of an individual and the last name of the individual in combination with 1 or more of the following categories of sensitive covered data, if either the name or the sensitive covered data are not encrypted or redacted:

(aa) A government-issued identifier described in section 101(49)(A)(i).

(bb) A financial account number described in section 101(49)(A)(iv).

(cc) Health information, but only to the extent such information reveals the history of medical treatment or diagnosis by a health care professional of the individual.

(dd) Biometric information.

(ee) Genetic information.

(D) LIMITATIONS ON DUAL ACTIONS.—Any amount that a court orders an entity to pay to a person under subparagraph (A)(i), (B), or (C) shall be offset by any amount the person received from an action brought against the entity for the same violation under section 115 or 116.

(b) OPPORTUNITY TO CURE IN ACTIONS FOR INJUNCTIVE RELIEF.—

(1) NOTICE.—Subject to paragraph (3), an action for injunctive relief may be brought by a person under this section only if, prior to initiating such action against an entity, the person provides to the entity written notice identifying the specific provisions of this title the person alleges have been or are being violated.

(2) EFFECT OF CURE.—In the event a cure is possible with respect to a violation alleged in a notice described in paragraph (1) and, not later than 60 days after the date of receipt of such notice, the entity cures such violation and provides the person an express written statement that the violation has been cured and that no further such violations shall occur, an action for injunctive relief may not be permitted with respect to the noticed violation.

(3) INJUNCTIVE RELIEF FOR A SUBSTANTIAL PRIVACY HARM.—Notice is not required under paragraph (1) prior to bringing an action for injunctive relief for a violation that resulted in a substantial privacy harm.

(c) NOTICE OF ACTIONS SEEKING ACTUAL DAMAGES.—

(1) NOTICE.—Subject to paragraph (4), an action under this section for actual damages may be brought by a person only if, 60 days prior to initiating such action against an entity, the person provides the entity written notice identifying the specific provisions of this title the person alleges have been or are being violated.

(2) SETTLEMENT.—An entity that receives a written notice from a person under paragraph (1) may settle with the person who sent the written notice.

(3) EFFECT OF SETTLEMENT.—In the event of a settlement under paragraph (2), the terms of such settlement shall govern any future action under this section for actual damages between the parties to the settlement that relates to the underlying facts that resulted in the settlement.

(4) NO NOTICE REQUIRED FOR A SUBSTANTIAL PRIVACY HARM.—Notice is not required under paragraph (1) prior to bringing an action for actual damages for a violation of this title that resulted in a substantial privacy harm, if such action includes a claim for a preliminary injunction or temporary restraining order.

(d) PRE-DISPUTE ARBITRATION AGREEMENTS.—

(1) IN GENERAL.—Notwithstanding any other provision of law, at the election of the person alleging a violation of this title, no pre-dispute arbitration agreement shall be valid or enforceable with respect to—

(A) a claim alleging a violation involving an individual under the age of 18; or

(B) a claim alleging a violation that resulted in a substantial privacy harm.

(2) DETERMINATION OF APPLICABILITY.—Any issue as to whether this subsection applies to a dispute shall be determined under Federal law. The applicability of this subsection to an agreement to arbitrate and the validity and enforceability of an agreement to which this subsection applies shall be determined by a Federal court, rather than an arbitrator, irrespective of whether the party resisting arbitration challenges the arbitration agreement specifically or in conjunction with other terms of the contract containing the agreement, and

irrespective of whether the agreement purports to delegate the determination to an arbitrator.

(3) PRE-DISPUTE ARBITRATION AGREEMENT DEFINED.—For purposes of this subsection, the term "pre-dispute arbitration agreement" means any agreement to arbitrate a dispute that has not arisen at the time of the making of the agreement.

(e) COMBINED NOTICES.—A person may combine the notices required by subsections (b)(1) and (c)(1) into a single notice, if the single notice complies with the requirements of each such subsection.

(f) BAD FAITH.—If a person represented by counsel brings a civil action under this section against a covered entity or service provider requesting actual damages from the covered entity or service provider, and fails to provide notice to the covered entity or service provider in accordance with this section, the action may be dismissed without prejudice and may not be reinstated until the person has complied with the notice requirements of this section.

SEC. 118. RELATION TO OTHER LAWS.

(a) PREEMPTION OF STATE LAWS.—

(1) CONGRESSIONAL INTENT.—The purposes of this section are to—

(A) establish a uniform national privacy and data security standard in the United States to prevent administrative costs and burdens from being placed on interstate commerce; and

(B) expressly preempt the laws of a State or political subdivision of a State as provided in this subsection.

(2) PREEMPTION.—Except as provided in paragraphs (3) and (4), no State or political subdivision of a State may adopt, maintain, enforce, impose, or continue in effect any law, regulation, rule, requirement, prohibition, standard, or other provision covered by the provisions of this title or a rule, regulation, or requirement promulgated under this title.

(3) STATE LAW PRESERVATION.—Paragraph (2) may not be construed to preempt, displace, or supplant the following State laws, rules, regulations, or requirements:

(A) Consumer protection laws of general applicability, such as laws regulating deceptive, unfair, or unconscionable practices.

(B) Civil rights laws.

(C) Provisions of laws that address the privacy rights or other protections of employees or employee information.

(D) Provisions of laws that address the privacy rights or other protections of students or student information.

(E) Provisions of laws, insofar as such provisions address notification requirements in the event of a data breach.

(F) Contract or tort law.

(G) Criminal laws.

(H) Civil laws regarding—

(i) blackmail;

(ii) stalking (including cyberstalking);

(iii) cyberbullying;

(iv) intimate images (whether authentic or computer-generated) known to be nonconsensual;

(v) child abuse;

(vi) child sexual abuse material;

(vii) child abduction or attempted child abduction;

(viii) child trafficking; or

(ix) sexual harassment.

(I) Public safety or sector-specific laws unrelated to privacy or data security, but only to the extent such laws do not directly conflict with the provisions of this title.

(J) Provisions of laws that address public records, criminal justice information systems, arrest records, mug shots, conviction records, or non-conviction records.

(K) Provisions of laws that address banking records, financial records, tax records, Social Security numbers, credit cards, identity theft, credit reporting and investigations, credit repair, credit clinics, or check-cashing services.

(L) Provisions of laws that address electronic surveillance, wiretapping, or telephone monitoring.

(M) Provisions of laws that address unsolicited email messages, telephone solicitation, or caller identification.

(N) Provisions of laws that protect the privacy of health information, healthcare information, medical information, medical records, HIV status, or HIV testing.

(O) Provisions of laws that address the confidentiality of library records.

(P) Provisions of laws that address the use of encryption as a means of providing data security.

(4) ADDITIONAL PREEMPTION LIMITATIONS.—Notwithstanding paragraph (2), the provisions of this title shall preempt any State law, rule, or regulation that provides protections for children or teens 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.

(b) FEDERAL LAW PRESERVATION.—

(1) IN GENERAL.—Nothing in this title or a regulation promulgated under this title may be construed to limit—

(A) the authority of the Commission, or any other Executive agency, under any other provision of law;

(B) any requirement for a common carrier subject to section 64.2011 of title 47, Code of Federal Regulations (or any successor regulation), regarding information security breaches; or

(C) any other provision of Federal law, except as otherwise provided in this title.

(2) ANTITRUST SAVINGS CLAUSE.—

(A) ANTITRUST LAWS DEFINED.—For purposes of this paragraph, the term "antitrust laws"—

(i) has the meaning given such term in subsection (a) of the first section of the Clayton Act (15 U.S.C. 12(a)); and

(ii) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45), to the extent such section applies to unfair methods of competition.

(B) FULL APPLICATION OF THE ANTITRUST LAWS.—Nothing in this title or a regulation promulgated under this title may be construed to modify, impair, supersede the operation of, or preclude the application of the antitrust laws.

(3) APPLICATION OF OTHER FEDERAL PRIVACY AND DATA SECURITY REQUIREMENTS.—

(A) IN GENERAL.—To the extent that a covered entity or service provider is required to comply with any Federal law or regulation described in subparagraph (B), such covered entity or service provider is not subject to this title with respect to the activities governed by the requirements of such law or regulation.

(B) LAWS AND REGULATIONS DESCRIBED.—The Federal laws and regulations described in this subparagraph are the following:

(i) Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).

(ii) Part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.).

(iii) Subtitle D of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17921 et seq.).

(iv) The regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note).

(v) The requirements regarding the confidentiality of substance use disorder information under section 543 of the Public Health Service Act (42 U.S.C. 290dd–2) or any regulation promulgated under such section.

(vi) The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(vii) Section 444 of the General Education Provisions Act (commonly known as the "Family Educational Rights and Privacy Act of 1974") (20 U.S.C. 1232g) and part 99 of title 34, Code of Federal Regulations (or any successor regulation), to the extent a covered entity or service provider is an educational agency or institution (as defined in

such section or section 99.3 of title 34, Code of Federal Regulations (or any successor regulation)).

(viii) The regulations related to the protection of human subjects under part 46 of title 45, Code of Federal Regulations.

(x) The Health Care Quality Improvement Act of 1986 (42 U.S.C. 11101 et seq.).

(xi) Part C of title IX of the Public Health Service Act (42 U.S.C. 299b–21 et seq.).

(xii) Chapter 123 of title 18, United States Code.

(C) IMPLEMENTATION GUIDANCE.—Not later than 1 year after the date of the enactment of this Act, the Commission shall issue guidance with respect to the implementation of this paragraph.

(c) PRESERVATION OF COMMON LAW OR STATUTORY CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this title, nor any amendment, standard, rule, requirement, assessment, or regulation promulgated under this title, may be construed to preempt, displace, or supplant any Federal or State common law rights or remedies, or any State statute creating a remedy for civil relief, including any cause of action for personal injury, wrongful death, property damage, or other financial, physical, reputational, or psychological injury based in negligence, strict liability, products liability, failure to warn, an objectively offensive intrusion into the private affairs or concerns of an individual, or any other legal theory of liability under any Federal or State common law, or any State statutory law, except that the fact of a violation of this title or a regulation promulgated under this title may not be pleaded as an element of any violation of such law.

(d) NONAPPLICATION OF CERTAIN PROVISIONS OF COMMUNICATIONS ACT OF 1934 AND TELECOMMUNICATIONS ACT OF 1996 RELATED TO FCC PRIVACY AND DATA SECURITY LAWS AND REGULATIONS.—

(1) IN GENERAL.—Except as provided in paragraph (2), sections 201, 202, 222, 338(i), and 631 of the Communications Act of 1934 (47 U.S.C. 201; 202; 222; 338(i); 551) and section 706 of the Telecommunications Act of 1996 (47 U.S.C. 1302), and any regulation or order issued by the Federal Communications Commission under any such section, do not apply to any covered entity or service provider with respect to the collection, processing, retention, transfer, or security of covered data (or the equivalent of such data), to the extent that such sections or any regulation or order issued under such sections would otherwise cover the collection, processing, retention, transfer, or security of covered data (or the equivalent of such data) in order to protect consumer privacy or the security of such data, and a covered entity or service provider shall instead be covered by the

requirements of this title with respect to the collection, processing, retention, transfer, and security of covered data.

(2) EXCEPTIONS.—Paragraph (1) does not supersede any authority of the Federal Communications Commission with respect to the following:

(A) Emergency services (as defined in section 7 of the Wireless Communications and Public Safety Act of 1999 (47 U.S.C. 615b)).

(B) Proceedings to implement section 227 of the Communications Act of 1934 (47 U.S.C. 227) or the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (Public Law 116–105; 133 Stat. 3274), or any other authority used by the Federal Communications Commission to prevent or reduce unwanted telephone calls or text messages.

(C) An enforcement action alleging or finding a violation of a section of the Communications Act of 1934 specified in paragraph (1), if such action was adopted by the Federal Communications Commission prior to the date of the enactment of this Act.

(D) Subsection (a) of section 222 of the Communications Act of 1934 (47 U.S.C. 222), to the extent such subsection imposes a duty on every telecommunications carrier to protect the confidentiality of proprietary information of, and relating to, other telecommunications carriers and equipment manufacturers.

(E) Subsections (b), (d), and (g) of section 222 of the Communications Act of 1934 (47 U.S.C. 222).

(F) Any obligation of an international treaty related to the exchange of traffic implemented and enforced by the Federal Communications Commission.

SEC. 119. CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998.

Nothing in this title may be construed to relieve or change any obligation that a covered entity or other person may have under the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.).

SEC. 120. DATA PROTECTIONS FOR COVERED MINORS.

(a) PROHIBITION ON TARGETED AND FIRST-PARTY ADVERTISING TO COVERED MINORS.—A covered entity or service provider acting on behalf of a covered entity may not engage in targeted advertising or first-party advertising to an individual if the covered entity has knowledge that the individual is a covered minor, except that a covered entity or service provider may present or display to a covered minor age-appropriate advertisements intended for an audience of covered minors, if the covered entity or service provider does not use any covered data in relation to such

advertisements, other than data relating to the status of the individual as a covered minor.

(b) DATA TRANSFER REQUIREMENTS RELATED TO COVERED MINORS.—

(1) IN GENERAL.—Except as provided in paragraph (2), and notwithstanding section 102(b), a covered entity or a service provider acting on behalf of a covered entity may not transfer or direct a service provider to transfer the covered data of an individual to a third party if the covered entity—

(A) has knowledge that the individual is a covered minor; and

(B) has not obtained affirmative express consent, unless the transfer is necessary, proportionate, and limited to a purpose expressly permitted by paragraph (2), (3), (4), (8), (9), (11), (12), or (13) of section 102(d).

(2) EXCEPTION.—A covered entity or service provider may collect, process, retain, or transfer covered data of an individual that the covered entity or service provider knows is a covered minor in order to submit information relating to child victimization to law enforcement or to the nonprofit, national resource center and clearinghouse congressionally designated to provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children issues.

(c) RULEMAKING.—The Commission may conduct a rulemaking pursuant to section 553 of title 5, United States Code, to establish processes for parents and teens to exercise the rights provided in this title with respect to covered entities and data brokers. Any such rulemaking shall take into account—

(1) the specific needs of parents, children, and teens;

(2) how best to harmonize the processes provided for under this title with the processes and guidance provided for under the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.), as amended by title II of this Act, and any regulations promulgated by the Commission thereunder; and

(3) options for reducing undue burdens on parents, children, teens, covered entities, and data brokers.

SEC. 121. TERMINATION OF FTC RULEMAKING ON COMMERCIAL SURVEILLANCE AND DATA SECURITY.

Beginning on the date of the enactment of this Act, the rulemaking proposed in the advance notice of proposed rulemaking titled "Trade Regulation Rule on Commercial Surveillance and Data Security" and published on August 22, 2022 (87 Fed. Reg. 51273) shall be terminated.

SEC. 122. SEVERABILITY.

If any provision of this title, or the application thereof to any person or circumstance, is held invalid, the remainder of this title, and the application of such provision to other persons not similarly situated or to other circumstances, may not be affected by the invalidation.

SEC. 123. INNOVATION RULEMAKINGS.

The Commission may conduct a rulemaking pursuant to section 553 of title 5, United States Code—

(1) to include other covered data in the definition of the term "sensitive covered data", except that the Commission may not expand the category of information described in section 101(49)(A)(ii); and

(2) to include in the list of permitted purposes in section 102(d) other permitted purposes for collecting, processing, retaining, or transferring covered data.

SEC. 124. EFFECTIVE DATE.

Unless otherwise specified in this title, this title shall take effect on the date that is 180 days after the date of the enactment of this Act.

TITLE II—CHILDREN'S ONLINE PRIVACY PROTECTION ACT 2.0

SEC. 201. SHORT TITLE.

This title may be cited as the "Children's Online Privacy Protection Act 2.0".

SEC. 202. ONLINE COLLECTION, USE, DISCLOSURE, AND DELETION OF PERSONAL INFORMATION OF CHILDREN.

(a) DEFINITIONS.—Section 1302 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501) is amended—

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

"(2) OPERATOR.—The term 'operator'—

"(A) 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); and

"(B) 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).";

(2) in paragraph (4)—

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

"(A) the release of personal information collected from a child 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 a website, online service, online application, or mobile application (as defined in paragraph (8)(C)) of the operator, excluding any activity relating to targeted advertising or first-party advertising (as such terms are defined in section 101 of the American Privacy Rights Act of 2024) to children; and

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

(B) in subparagraph (B)—

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

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

(3) 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 e-mail 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 over time and across different websites, online services, online applications, or mobile applications, including a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or a unique device identifier, but excluding an identifier that is used by an operator solely for providing support for the internal operations of a website, online service, online application, or mobile application;

"(viii) a photograph, video, or audio file, if such file contains the image or voice of a specific child;

"(ix) geolocation information;

"(x) information generated from the measurement or technological processing of the biological, physical, or physiological characteristics of an individual 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 (DNA) information; or

"(VI) gait; or

"(xi) information linked or reasonably linkable to a child or the parents of that child (including any unique identifier) that an operator

collects online from the child and combines with an identifier described in this subparagraph.

"(B) EXCLUSION.—The term 'personal information' does not include an audio file that contains the voice of a child, if the operator—

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

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

"(iii) 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, such as 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) 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 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 targeted advertising or first-party advertising (as such terms are defined in section 101 of the American Privacy Rights Act of 2024) to children, 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.";

(4) by amending 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 a parent of the child—

"(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 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.";

(5) in paragraph (10)—

(A) 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";

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

(C) by adding at the end the following new subparagraph:

"(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

(6) by adding at the end the following:

"(13) CONNECTED DEVICE.—The term 'connected device' has the meaning given such term in section 101 of the American Privacy Rights Act of 2024.

"(14) EDUCATIONAL AGENCY OR INSTITUTION.—The term 'educational agency or institution' means a State educational agency or local educational agency as defined under Federal law, as well as an institutional day or residential school, including a public school, charter school, or private school, that provides elementary or secondary education, as determined under State law.

"(15) MOBILE APPLICATION.—The term 'mobile application' has the meaning given such term in section 101 of the American Privacy Rights Act of 2024.

"(16) ONLINE APPLICATION.—The term 'online application' has the meaning given such term in section 101 of the American Privacy Rights Act of 2024.

"(17) PRECISE GEOLOCATION INFORMATION.—The term 'precise geolocation information' has the meaning given such term in section 101 of the American Privacy Rights Act of 2024.".

(b) ONLINE COLLECTION, USE, DISCLOSURE, AND DELETION OF PERSONAL INFORMATION OF CHILDREN.—Section 1303 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6502) is amended—

(1) by striking the heading and inserting the following: "**ONLINE COLLECTION, USE, DISCLOSURE, AND DELETION OF PERSONAL INFORMATION OF CHILDREN**.";

(2) by amending subsection (a) to read as follows:

"(a) ACTS PROHIBITED.—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—

"(1) to collect personal information from a child in a manner that violates the American Privacy Rights Act of 2024 or the regulations prescribed under

subsection (b); or

"(2) to store or transfer the personal information of a child outside of the United States, unless—

"(A) the operator provides direct notice to the parent of the child that the personal information of the child is being stored or transferred outside of the United States; and

"(B) with respect to transfer, the operator meets the requirements of section 102(b) of the American Privacy Rights Act of 2024.";

(3) in subsection (b)—

(A) in paragraph (1)—

(i) in subparagraph (A)—

(I) in the matter preceding clause (i), 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";

(II) in clause (i)—

(aa) by striking "notice on the website" and inserting "clear and conspicuous notice on the website, service, or application"; and

(bb) by striking "; and" and inserting a semicolon;

(III) in clause (ii)—

(aa) by striking "verifiable parental consent" and inserting "verifiable consent"; and

(bb) by striking the semicolon at the end and inserting "; and"; and

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

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

(ii) by striking subparagraph (B);

(iii) in subparagraph (C)—

(I) by striking "reasonably"; and

(II) by inserting ", proportionate, and limited" after "necessary";

(iv) in subparagraph (D), by striking "website or online service" and inserting "website, online service, online application, or mobile application"; and

(v) by redesignating subparagraphs (C) and (D) as subparagraphs (B) and (C), respectively;

(B) in paragraph (2)—

(i) in the matter preceding subparagraph (A)—

(I) by striking "verifiable parental consent" and inserting "verifiable consent"; and

(II) by striking "paragraph (1)(A)(ii)" and inserting "clause (ii) or (iii) of paragraph (1)(A)";

(ii) in subparagraph (A), by inserting "or to contact another child" after "to recontact the child";

(iii) in subparagraph (B)—

(I) by striking "or child"; and

(II) by striking "parental consent" each place the term appears and inserting "verifiable consent";

(iv) in subparagraph (D), in the matter preceding clause (i)—

(I) by striking "reasonably"; and

(II) by inserting ", proportionate, and limited" after "necessary"; and

(v) in subparagraph (E)—

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

application, or mobile application"; and

(II) in clause (i), by striking "website" and inserting "website, service, or application";

(C) by redesignating paragraph (3) as paragraph (4) and inserting after paragraph (2) the following new paragraph:

"(3) APPLICATION TO OPERATORS ACTING UNDER AGREEMENTS WITH EDUCATIONAL AGENCIES OR INSTITUTIONS.—The regulations may provide that verifiable consent under clause (ii) or (iii) of paragraph (1)(A) is not required for an operator that is acting under a written agreement with an educational agency or institution that, at a minimum, requires—

"(A) the operator to—

"(i) limit its collection, use, and disclosure of the personal information from a child 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, 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 online notice of information practices of the operator as required under paragraph (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, to prevent further use or maintenance or future collection of personal information from a child, and to delete personal information collected from a child or content or information submitted by a child to the website, online service, online application, or mobile application of the operator;

"(B) a representative of the educational agency or institution to—

"(i) acknowledge and agree that the representative has authority to authorize the collection, use, and disclosure of personal information from children on behalf of the educational agency or institution; and

"(ii) provide the name of the representative and the title of the representative at the educational agency or institution; and

"(C) the educational agency or institution to—

"(i) provide on the website of the educational agency or institution a notice that identifies the operator with which the educational agency or institution has entered into a written agreement under this paragraph and a link to the online notice of information practices of the operator as required under paragraph (1)(A)(i);

"(ii) provide the notice of the operator regarding the information practices of the operator, as required under subparagraph (A)(ii), upon request, to a parent; and

"(iii) upon the request of a parent, request the operator provide a means to review the personal information collected from the child of the parent and provide the parent a means to review the personal information.";

(D) 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 requested to delete covered data of the child pursuant to section 105 of the American Privacy Rights Act of 2024."; and

(E) by adding at the end the following new paragraphs:

"(5) CONTINUATION OF SERVICE.—The regulations shall prohibit an operator from discontinuing service provided to a child on the basis of a request by the parent of the child to delete personal information collected from the child, to the extent that the operator is capable of providing such service without such information.

"(6) COMMON VERIFIABLE CONSENT MECHANISM.—

"(A) IN GENERAL.—

"(i) FEASIBILITY OF MECHANISM.—The Commission shall conduct an assessment, with notice and public comment, of the feasibility 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 on behalf of multiple, listed operators that provide a joint or related service.

"(B) REPORT.—Not later than 1 year after the date of the enactment of this paragraph, 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 with the findings of the assessment required by subparagraph (A).

"(C) REGULATIONS.—If the Commission finds, in the assessment required by subparagraph (A), that the use of a common verifiable consent mechanism is feasible and would meet the requirements of this title, the Commission shall issue regulations, pursuant to section 553 of title 5, United States Code, to permit the use of a common verifiable consent mechanism in accordance with the findings outlined in the report submitted under subparagraph (B).";

(4) in subsection (c), by striking "a regulation prescribed under subsection (a)" and inserting "paragraph (2) of subsection (a), or of a regulation prescribed under subsection (b),"; and

(5) 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 may be construed to prohibit any State from enacting a law, rule, or regulation that provides greater protection to children than the provisions of this title.".

(c) SAFE HARBORS.—Section 1304 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6503) is amended 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 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 sections 6(f) and 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).".

(d) ACTIONS BY STATES.—Section 1305 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6504) is amended—

(1) in subsection (a)(1)—

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

(B) in subparagraph (B), by striking "the regulation" and inserting "such section or regulation"; and

(2) in subsection (d)—

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

(B) by striking "that regulation" and inserting "such section or regulation".

(e) ADMINISTRATION AND APPLICABILITY OF ACT.—Section 1306 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6505) is amended—

(1) in subsection (d)—

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

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

(2) by adding at the end the following new subsections:

"(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, the Commission or a State attorney 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. Nothing in this title, including a determination described in the preceding sentence, may be construed to require an operator to—

"(A) affirmatively collect any personal information with respect to the age of a child that an operator is not already collecting in the normal course of business; or

"(B) implement an age gating or age verification functionality.

"(2) COMMISSION GUIDANCE.—

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

"(B) LIMITATION.—No guidance issued by the Commission under subparagraph (A) confers any rights on any person, State, or locality, or operates to bind the Commission or any person, State, or locality 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, and 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.

"(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 per chapter 6 of title 5, United States Code.".

SEC. 203. STUDY AND REPORTS ON MOBILE AND ONLINE APPLICATION OVERSIGHT AND ENFORCEMENT.

(a) OVERSIGHT REPORT.—Not later than 3 years after the date of the enactment of this Act, the Federal Trade 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 on the processes of platforms that offer mobile and online applications for ensuring that, for those applications that are websites, online services, online applications, or mobile applications directed to children, the applications operate in accordance with—

(1) this title, the amendments made by this title, and any rules promulgated under this title or the amendments made by this title; and

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

(b) ENFORCEMENT REPORT.—Not later than 1 year after the date of the enactment of this Act, and annually thereafter, the Federal Trade 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 addresses, at a minimum—

(1) the number of actions brought by the Commission during the reporting year to enforce the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.) and the outcome of each such action;

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

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

(4) 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

(5) policy or legislative recommendations to strengthen online protections for children.

(c) Report By The Inspector General.—

(1) IN GENERAL.—Not later than 2 years after the date of the enactment of this Act, the Inspector General of the Federal Trade Commission shall submit to the Federal Trade 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 children; 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.

SEC. 204. SEVERABILITY.

If any provision of this title or the amendments made by this title, or the application thereof to any person or circumstance, is held invalid, the remainder of this title and the amendments made by this title, and the application of such provision to other persons not similarly situated or to other circumstances, may not be affected by the invalidation.