Title: To establish protections for covered data of individuals, 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:

SEC. 2. DEFINITIONS.

In this Act:

(1) AFFIRMATIVE EXPRESS CONSENT.—

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

(i) clearly communicates the individual's authorization for an act or practice;

(ii) is in response to a specific request from a covered entity, or service provider on behalf of a covered entity; and

(iii) meets the requirements of subparagraph (B).

(B) REQUEST REQUIREMENTS.—The requirements of this subparagraph, with respect to a request made under subparagraph (A), 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 individual's consent is sought and—

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

(II) clearly states the specific categories of covered data that the covered entity shall collect, process, retain, or transfer to fulfill the request; and

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

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

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

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

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

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

(2) BIOMETRIC INFORMATION.—

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

(i) fingerprints;

(ii) voice prints;

(iii) iris or retina imagery scans;

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

(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) metadata associated with a digital or physical photograph or an audio or video recording that cannot be used to identify an individual.

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

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

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

(6) CONNECTED DEVICE.—The term "connected device" means a device that is capable of connecting to the internet over a fixed or wireless connection.

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

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

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

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

(8) COVERED ALGORITHM.—The term "covered algorithm" means a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision-making by using covered data, which includes determining the provision of products or services or ranking, ordering, promoting, recommending, amplifying, or similarly determining the delivery or display of information to an individual.

(9) COVERED DATA.—

(A) IN GENERAL.—The term "covered data" means information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to 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 provided that such inferences—

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

(II) are not combined with covered data; or

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

(I) a collection that is open to the public or routinely made available to researchers who are not affiliated with the library, archive, or museum;

(II) a public service mission;

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

(IV) collections composed of lawfully acquired materials and all licensing conditions for such materials are met.

(10) COVERED ENTITY.—

(A) IN GENERAL.—The term "covered entity"—

(i) 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. 201–231) as currently enacted or subsequently amended; or

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

(ii) includes any entity that controls, is controlled by, is under common control with, or shares common branding with another covered entity; and

(iii) does not include—

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

(II) an entity that is collecting, processing, retaining, or transferring covered data on behalf of a Federal, State, Tribal, territorial, 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) the National Center for Missing and Exploited Children; or

(V) except with respect to the obligations under section 9, a nonprofit organization whose primary mission is to prevent, investigate, or deter fraud or to train anti-fraud professionals or 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.

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

(11) COVERED HIGH-IMPACT SOCIAL MEDIA COMPANY.—The term "covered high-impact social media company" means a covered entity that provides any internet-accessible platform where—

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

(B) such platform has 300,000,000 or more global monthly active users for not fewer than 3 of the preceding 12 months on the platform of such covered entity; and

(C) such platform constitutes an online product or service that is primarily used by individuals to access or share user-generated content.

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

(13) 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 such covered data.

(B) PRINCIPAL SOURCE OF REVENUE DEFINED.—For purposes of this paragraph, the term "principal source of revenue" means, with respect to the preceding 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 or transferring the covered data of more than 5,000,000 individuals that the covered entity did not collect directly from the individuals linked or linkable to the covered data.

(C) 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.

(14) 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.

(15) DE-IDENTIFIED DATA.—The term "de-identified data" means—

(A) information that cannot reasonably be used to infer or derive the identity of an individual, 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 such individual, regardless of whether the information is aggregated, provided that the covered entity or service provider—

(i) takes reasonable physical, administrative, or 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; and

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

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

(II) require that such contractual obligations be included in all subsequent instances for which the data may be received; or

(B) health information (as defined in section 262 of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d)) that has been de-identified in accordance with section 164.514(b) of title 45, Code of Federal Regulations, provided 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 must comply with clauses (ii) and (iii) of subparagraph (A) for the information to be considered de-identified under this Act.

(16) DERIVED DATA.—The term "derived data" means covered data that is created by the derivation of information, data, assumptions, correlations, inferences, predictions, or conclusions from facts, evidence, or another source of information or data about an individual or an individual's device.

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

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

(19) EMPLOYEE INFORMATION.—The term "employee information" means covered data, biometric information, or genetic information that is collected by a covered entity (or a service provider acting on behalf of a covered entity)—

(A) about an individual in the course of the individual's employment or application

for employment (including on a contract or temporary basis), provided that such data is retained or processed by the covered entity or the service provider solely for purposes necessary for the individual's employment or application for employment;

(B) that is emergency contact information for an individual who is an employee or job applicant of the covered entity, provided that such data is retained or processed by the covered entity or the service provider solely for the purpose of having an emergency contact for such individual on file; or

(C) about an individual (or a relative of an individual) who is an employee or former employee of the covered entity for the purpose of administering benefits to which such individual or relative is entitled on the basis of the individual's employment with the covered entity, provided that such data is retained or processed by the covered entity or the service provider solely for the purpose of administering such benefits.

(20) ENTITY.—The term "entity" means an individual, trust, partnership, association, organization, company, or corporation.

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

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

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

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

(23) 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 or treatment of an individual, including the precise geolocation information of such treatment.

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

(25) 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) 15,000,000 portable connected devices that identify or are linked or reasonably linkable to 1 or more individuals; and

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

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

(B) EXCLUSIONS.—For purposes of subparagraph (A), a covered entity or service provider shall not be considered a large data holder solely on account 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 strictly necessary to initiate, render, bill for, finalize, complete, or otherwise facilitate payments for goods or services.

(C) DEFINITION OF ANNUAL GROSS REVENUE.—For 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.

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

(A) integrated into any product or service;

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

(C) used for targeted advertising or to otherwise market to any individual or individual's device.

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

(28) ON-DEVICE DATA.—The term "on-device data" means data stored under the sole control of an individual, including on an individual's device, and only to the extent such data is not processed or transferred by a covered entity or service provider.

(29) 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.

(30) PRECISE GEOLOCATION INFORMATION.—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—

(A) street-level location information of such individual or device; or

(B) the location of such individual or device within a range of 1,850 feet or less.

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

(32) 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 from—

(i) Federal, State, or local government records provided that 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.

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

(iii) OTHER LIMITATIONS.—The term "publicly available information" does not include any of the following:

(I) Any obscene visual depiction (as defined for purposes of 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 sensitive covered data.

(III) Biometric information.

(IV) Genetic information.

(V) Covered data that has been combined with publicly available information.

(VI) Intimate images, authentic or generated by a computer or by artificial intelligence, known to be nonconsensual.

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

(34) SENSITIVE COVERED DATA.—

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

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

(ii) Any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare condition 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.

(v) Biometric information.

(vi) Precise geolocation information.

(vii) An individual's private communications, such as voicemails, emails, texts, direct messages, or mail, or information identifying the parties to such communications, information contained in telephone bills, voice communications, and any information that pertains to the transmission of voice 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 covered entity is an intended recipient of the communication.

(viii) Account or device log-in credentials.

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

(x) Calendar information, address book information, phone or text logs, photos, 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 any individual's access, viewing, or other use of any video programming described in section 713(b)(2) of the Communications Act of 1934 (47 U.S.C. 613(h)(2)), including 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 data 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 data used solely for transfers for independent video measurement).

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

(xv) Information revealing an individual's online activities over time and across websites or online services that do not share common branding or over time on any website or online service operated by a covered high-impact social media company.

(xvi) Information about an individual who is a covered minor.

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

(xviii) Any other covered data, except for expanding the categories described in clause (ii), that the Commission determines to be sensitive covered data through a rulemaking pursuant to section 553 of title 5, United States Code.

(B) THIRD PARTY.—For 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, cable service, satellite service, or streaming media service; and

(ii) provides video programming as described in subparagraph (A)(xii).

(35) 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, a covered 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 data if the entity, jointly or with others, determines the purposes and means of the

specific collecting, processing, retaining, or transferring of data.

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

(36) SMALL BUSINESS.—

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

(i) whose average annual gross revenues for the period of the 3 preceding calendar years (or for the period during which the covered entity has been in existence if such period is less than 3 years) did not exceed $40,000,000;

(ii) that, on average, 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, so long as all covered data for such purpose was deleted or de-identified within 90 days, except when necessary to investigate fraud or as consistent with a covered entity's return or warranty policy; and

(iii) that did not transfer covered data to a third party in exchange for revenue or anything of value.

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

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

(38) 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.

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

(A) means displaying or presenting to an individual or device identified by a unique persistent identifier (or group of individuals or devices identified by unique persistent

identifiers) an online advertisement that is selected based on known or predicted preferences or interests associated with the individual or device identified by a unique identifier; and

(B) does not include—

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

(ii) first-party advertising based on an individual's visit to or use of a website or online service that offers a product or service that is related to the subject of the advertisement;

(iii) contextual advertising when an advertisement is displayed online based on the content of the webpage or online service on which the advertisement appears; or

(iv) processing covered data solely for measuring or reporting advertising, marketing, or media performance, reach, or frequency, including by independent entities.

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

(A) means any entity that—

(i) receives covered data from another entity; 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 related by common ownership or corporate control and share common branding.

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

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

(43) UNIQUE PERSISTENT IDENTIFIER.—The term "unique persistent identifier" means—

(A) a technologically created identifier to the extent that such identifier is reasonably linkable to an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals, including a device identifier, an Internet Protocol address, cookies, beacons, pixel tags, mobile ad identifiers, or similar technology, customer number, unique pseudonym, or user alias, telephone numbers, or other forms of persistent or probabilistic identifiers that are linked or reasonably linkable to 1 or more individuals or devices; and

(B) does not include an identifier assigned by a covered entity for the specific purpose of giving effect to an individual's exercise of affirmative express consent or opt-out of the collection, processing, retaining, or transfer of covered data or otherwise limiting the collection, processing, retaining, or transfer of such information.

(44) WIDELY DISTRIBUTED MEDIA.—The term "widely distributed media"—

(A) 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; and

(B) does not include an obscene visual depiction (as defined in section 1460 of title 18, United States Code).

SEC. 3. DATA MINIMIZATION.

(a) In General.—Subject to subsections (b) and (c), a covered entity, or a service provider acting on behalf of a covered entity, shall not collect, process, retain, or transfer covered data—

(1) beyond what is necessary, proportionate, and limited 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 by the covered entity to the individual reasonably anticipated within the context of the relationship; or

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

(b) Sensitive Covered Data.—

(1) IN GENERAL.—Except as expressly provided under subsection (d), a covered entity, or a service provider acting on behalf of a covered entity, shall not transfer sensitive covered data to a third party without the affirmative express consent of the individual to whom such data pertains.

(2) WITHDRAWAL OF AFFIRMATIVE EXPRESS CONSENT.—

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

(B) REQUIREMENTS.—The means to withdraw affirmative express consent described in subparagraph (A) 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.

(c) Additional Protections for Biometric Information and Genetic Information.—

(1) IN GENERAL.—A covered entity, or a service provider acting on behalf of a covered entity, shall not collect, process, or retain biometric information or genetic information without the affirmative express consent of the individual to whom such information pertains, unless such collection, processing, or retention is essential for a purpose expressly permitted under paragraphs (1) through (4) or paragraphs (9) through (13) of subsection (d).

(2) RETENTION.—A covered entity, or service provider acting on behalf of a covered entity, shall not retain biometric or genetic information beyond the point for which a purpose that an individual provided affirmative express consent under paragraph (1) has

been satisfied or within 3 years of the individual's last interaction with the covered entity or service provider, whichever occurs first, unless such retention is essential for a purpose expressly permitted under paragraphs (1) through (4) or paragraphs (9) through (13) of subsection (d).

(3) TRANSFER.—A covered entity, or service provider acting on behalf of a covered entity, shall not transfer biometric information or genetic information to a third party without the affirmative express consent of the individual to whom such information pertains, unless such transfer is essential for a purpose expressly permitted under paragraphs (2), (3), (4), (8), (9), (11), or (12) of subsection (d).

(4) WITHDRAWAL OF AFFIRMATIVE EXPRESS CONSENT.—

(A) IN GENERAL.—A covered entity shall provide an individual with a means to withdraw affirmative express consent previously provided by the individual with respect to the biometric information or genetic information of the individual.

(B) REQUIREMENTS.—The means to withdraw affirmative express consent described in subparagraph (A) 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.

(d) Permitted Purposes.—A covered entity, or service provider acting on behalf of a covered entity, may collect, process, retain, or transfer covered data for the following purposes, provided that the covered entity or service provider can demonstrate that the collection, processing, retention, or transferring is necessary, proportionate, and limited to such purpose:

(1) To protect data security (as described in section 9), protect against spam, and maintain networks and systems, including through diagnostics, debugging, and repairs.

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

(3) To investigate, establish, prepare for, exercise, or defend cognizable legal claims on its own behalf.

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

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

(6) To conduct market research.

(7) With respect to covered data previously collected in accordance with this Act, to process such data into de-identified data, including to—

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

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

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

(i) is in the public interest; and

(ii) adheres to all relevant laws and regulations governing such research, including regulations for the protection of human subjects.

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

(A) a notice describing such transfer, including the name of any entity receiving the individual's covered data and the privacy policies of such entity (as described in section 4); and

(B) a reasonable opportunity to—

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

(ii) request the deletion of the individual's covered data, as described in section 5.

(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 (as described in subparagraphs (A) and (C) of section 222(d)(4) of such Act (47 U.S.C. 222(d)(4)(A) and (C))).

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

(11) To prevent, detect, protect against, or respond to an ongoing or imminent network security or physical security incident, including an intrusion or trespass, medical alerts, fire alarms, or access control.

(12) To prevent, detect, protect against, or respond to an imminent or ongoing public safety incident (such 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, 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 Act, to process such data as necessary to provide first party or contextual advertising by the covered entity for individuals.

(15) Except with respect to sensitive covered data and only with respect to covered data previously collected in accordance with this Act, for an individual who has not opted out of targeted advertising pursuant to section 6, to process or transfer covered data to provide

targeted advertising.

(e) Guidance.—The Commission shall issue guidance regarding what is reasonably necessary and proportionate to comply with this section.

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

SEC. 4. TRANSPARENCY.

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

(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 the point of contact and a monitored email address, as applicable, for 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 retaining 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, including sensitive covered data, or, if it is not possible to identify that time frame, the criteria used to determine the length of time the covered entity or service provider intends to retain categories of covered data.

(5) A prominent description of how an individual can exercise the rights described in sections 5 and 6.

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

(7) The effective date of the privacy policy.

(8) 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 in part 7.4 of title 15, Code of Federal Regulations, or any successor regulation).

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

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

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

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

(e) Material Changes.—

(1) NOTICE AND OPT OUT.—A covered entity that makes a material change to its privacy policy or practices with respect to previously collected covered data 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 processing or transfer of such previously collected covered data 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 processing or transfer of such previously collected covered data, except if such processing or transfer is strictly necessary to provide a product or service specifically requested by the individual.

(2) DIRECT NOTIFICATION.—The covered entity shall take all reasonable electronic measures to provide direct notification, where possible, to each affected individual regarding material changes to the privacy policy, 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.

(3) CLARIFICATION.—Except as provided in paragraph (1)(B), nothing in this section shall be construed to affect the requirements for covered entities under section 3, 5, or 6.

(f) Transparency Requirements for Large Data Holders.—

(1) RETENTION OF PRIVACY POLICIES; LOG OF MATERIAL CHANGES.—Beginning after the date of enactment of this Act, each large data holder shall—

(A) retain and publish on the website of the large data holder a copy of each previous version of its privacy policy (as described in subsection (d)) for not less than 10 years; and

(B) make publicly available on its website, in a clear, conspicuous, and readily

accessible manner, a log that describes the date and nature of each material change to its privacy policy during such 10-year period in a manner that is sufficient for a reasonable individual to understand the effect of each material change.

(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 its covered data practices in a manner that—

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

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

(iii) 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

(iv) is not more than 500 words in length.

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

SEC. 5. INDIVIDUAL CONTROL OVER COVERED DATA.

(a) Access to, and Correction, Deletion, and Portability of, Covered Data.—Subject to subsections (b), (d), and (e), after receiving a verified request from an individual, a covered entity shall provide the individual with the right to—

(1) access—

(A) in a format that be naturally read by a human, the covered data of the individual (or an accurate representation of the covered data of the individual 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 of the individual, 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 the covered data of the individual to a third party or service provider;

(2) correct any inaccuracy or incomplete information with respect to the covered data of the individual that is collected, processed, or retained by the covered entity and, for covered data that has been transferred, notify any third party or service provider to which the covered entity transferred such covered data of the corrected information;

(3) delete covered data of the individual that is collected, processed, or 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 individual's deletion request; and

(4) to the extent technically feasible, export covered data (except for derived data if the export of such derived data would result in the release of trade secrets or other proprietary or confidential data) of the individual that is collected, processed, or retained by the covered entity without licensing restrictions that limit such transfers, in—

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

(B) a portable, structured, interoperable, and machine-readable format.

(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 times 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 time beyond the initial 3 times 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)—

(A) any large data holder or data broker shall comply with a verified request from an individual to exercise a right described in subsection (a) not later than 15 calendar days after receiving such request, unless it is impossible or demonstrably impracticable to verify such individual; and

(B) a covered entity that is not a large data holder shall comply with a verified request from an individual to exercise a right described in subsection (a) not later than 30 calendar days after receiving such request, unless it is impossible or demonstrably impracticable to verify such individual.

(2) EXTENSION.—The 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 the individual's requests, provided that the covered entity informs the individual of any such extension within the initial response period, together with the reason for the extension.

(d) Verification.—

(1) IN GENERAL.—A covered entity shall verify that any individual requesting to exercise a right described in subsection (a) is—

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

(B) an individual authorized to make such a request on the individual's behalf.

(2) ADDITIONAL INFORMATION.—If a covered entity cannot make the verification described in paragraph (1), the covered entity—

(A) may request that the individual making such request provide any additional information necessary for the sole purpose of verifying the identity of the individual; and

(B) shall not process, retain, or transfer such additional information for any other purpose.

(e) Exceptions.—

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

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

(B) determines that exercise of the right would require access to another individual's sensitive covered data;

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

(D) would violate Federal, State, local, or Tribal law that is not preempted by this Act;

(E) would violate the covered entity's professional ethical obligations;

(F) reasonably believes that the request is made in furtherance of 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.

(2) PERMISSIVE EXCEPTIONS.—

(A) IN GENERAL.—A covered entity may decline, with adequate explanation provided to the individual making the request, to comply with a request to exercise a right described in subsection (a), in whole or in part, if such compliance would—

(i) be demonstrably impossible due to technology or cost, and such adequate explanation includes a detailed description regarding the inability to comply with the request due to technology or cost;

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

(iii) 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;

(iv) prevent a covered entity from being able to maintain a confidential record of opt out requests pursuant to section 6, maintained solely for the purpose of preventing the covered data of an individual from being recollected after the individual submitted an opt out request; or

(v) with respect to deletion requests, require a private elementary or secondary school (as defined by State law) or a private institution of higher education (as defined by section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)) to delete covered data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution.

(B) PARTIAL COMPLIANCE.—In the event a covered entity makes a permissive exception under subparagraph (A), the covered entity shall partially comply with the remainder of the applicable request if partial compliance is possible and not unduly burdensome.

(C) NUMBER OF REQUESTS.—For purposes of subparagraph (A)(i), the receipt of a large number of verified requests, on its own, shall not be considered to render compliance with a request demonstrably impossible.

(3) RULE OF CONSTRUCTION.—This section shall not require a covered entity to—

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

(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 verified individual's request with the covered data that is the subject of the request.

(4) 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 necessary to protect the rights of individuals, alleviate undue burdens on covered entities, prevent unjust or unreasonable outcomes from the exercise of access, correction, deletion, or portability rights, or as otherwise necessary to fulfill the purposes of this section.

(B) CONSIDERATIONS.—In establishing such 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 not comply with an individual's request to exercise a right under this section for any purpose the Commission identifies pursuant to this paragraph.

(5) ON-DEVICE DATA EXEMPTION.—A covered entity may decline to comply with a request to exercise a right described in paragraph (1), (2), or (3) of subsection (a), in whole or in part, if—

(A) the covered data is exclusively on-device data; and

(B) the individual can exercise any such right using clear and conspicuous on-device controls.

(f) Large Data Holder Metrics Reporting.—With respect to each calendar year for which an entity is considered a large data holder, such entity shall comply with the following reporting requirements:

(1) REQUIRED METRICS.—Compile the following metrics for the prior 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 requests to opt-out of covered data transfers under section 6(a)(1).

(D) The number of requests to opt-out of targeted advertising under section 6(a)(2).

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

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

(2) PUBLIC DISCLOSURE.—Disclose by July 1 of each applicable calendar year the information compiled under paragraph (1)—

(A) in such large data holder's privacy policy; or

(B) on the publicly accessible website of such 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 enactment of this Act, the Commission shall issue guidance to clarify or explain the provisions of this section and establish processes 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 under subsection (a) in any language in which the covered entity provides a product or service.

(2) INDIVIDUALS WITH DISABILITIES.—The mechanisms by which a covered entity enables individuals to make requests under subsection (a) shall be readily accessible and usable by individuals with disabilities.

SEC. 6. OPT-OUT RIGHTS AND CENTRALIZED MECHANISM.

(a) In General.—Beginning on the effective date described in section 24, a covered entity shall provide to individuals the following opt-out rights:

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

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

(B) allow an individual to make an opt-out designation with respect to the transfer of the individual's covered data through an opt-out mechanism as described in subsection (b); and

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

(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 of covered data in furtherance of targeted advertising;

(B) allow an individual to make an opt-out designation with respect to targeted advertising through an opt-out mechanism as described in subsection (b); and

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

(b) Centralized Consent and Opt-out Mechanism.—

(1) IN GENERAL.—Not later than 2 years after the date of 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 a privacy protective, centralized mechanism (including global privacy signals such as browser or device privacy settings and registries of identifiers) 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 user friendly, clearly described, and easy to use by a reasonable individual;

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

(iii) clearly represents an individual's preference and is free of defaults constraining or presupposing such preference;

(iv) is provided in any language in which the covered entity provides products or services subject to the opt out;

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

(vi) does not conflict with other commonly-used privacy settings or tools that an individual may employ;

(B) provides a mechanism for the individual to selectively opt out of the covered entity's collection, processing, retention, or transfer of covered data, without affecting the individual's preferences 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 applies neutrally.

(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. 7. INTERFERENCE WITH CONSUMER RIGHTS.

(a) Dark Patterns Prohibited.—

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

(A) divert an individual's attention from any notice required under this Act;

(B) impair an individual's ability to exercise any right under this Act; or

(C) obtain, infer, or facilitate an individual's consent for any action that requires an individual's consent under this Act.

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

(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 Act through the use of any false, fictitious, fraudulent, or materially misleading statement or representation.

SEC. 8. 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 guaranteed by the Act, or any regulations promulgated under this Act, including denying products or services, charging different prices or rates for products or services, or providing a different level of quality of products 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) a different price, rate, level, quality, or selection of products or services to an individual, including offering products or services for no fee, if the offering is in connection with an individual's voluntary participation in a bona fide loyalty program, provided that—

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

(II) the covered entity provides an individual with means to withdraw the

affirmative express consent previously provided by the individual in the manner set forth in section 3(b)(2);

(III) the covered entity abides by an individual's exercise of any right described in sections 3(b)(2), 5, or 6; and

(IV) the individual provides affirmative express consent for the transfer of any data collected in connection with a bona fide loyalty program; and

(ii) different prices or functionalities with respect to a product or service based on an individual's decision to terminate membership in a bona fide loyalty program or to exercise a right under section 5(a)(3) that deletes covered data that is strictly necessary for participation in the bona fide loyalty program.

(B) BONA FIDE LOYALTY PROGRAM DEFINED.—For purposes of this paragraph, the term "bona fide loyalty program" includes rewards, premium features, discounts, or club card programs offered by a covered entity that is not 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 insofar as the collection and processing of covered data is strictly necessary for the function of such product or service.

SEC. 9. DATA SECURITY AND PROTECTION OF COVERED DATA.

(a) Establishment of Data Security Practices.—

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

(A) the confidentiality, integrity, and accessibility 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 covered entity's or the service provider's collecting, processing, retaining, or transferring of covered data, taking into account such covered entity's or service provider's changing business operations with respect to covered data;

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

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

(b) Specific Requirements.—The data security practices required under subsection (a) shall include, for each respective entity's own system, at a minimum, the following practices:

(1) ASSESS VULNERABILITIES.—Routinely identifying and assessing any reasonably foreseeable internal or external risk to, and 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 a plan to receive and consider unsolicited reports of vulnerability by any entity or individual, and, if such report is reasonably credible, perform a reasonable and timely investigation of such report and take appropriate action necessary to protect covered data against such vulnerability.

(2) PREVENTATIVE AND CORRECTIVE ACTION.—

(A) IN GENERAL.—Taking preventative and corrective action to mitigate any reasonably foreseeable internal or external risk or vulnerability to covered data identified by the covered entity or service provider, consistent with the nature of such risk or vulnerability and the covered entity's or service provider's role 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 technology, internal or external threats to covered data, and the covered entity's or service provider's changing business operations with respect to covered data.

(3) INFORMATION RETENTION AND DISPOSAL.—Disposing of covered data (either by or at the direction of a 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 an individual has provided affirmative express consent to such retention. Such disposal shall include destroying, permanently erasing, or otherwise modifying the covered data to make such data permanently unreadable or indecipherable and unrecoverable to ensure ongoing compliance with this section.

(4) RETENTION SCHEDULE.—Developing, maintaining, and adhering to a retention schedule for covered data disposal consistent with the practices and procedures required in 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 of data security.

(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. 10. EXECUTIVE RESPONSIBILITY.

(a) Designation of Privacy and Data Security Officers.—

(1) DESIGNATION.—

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

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

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

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

(2) REQUIREMENTS FOR LARGE DATA HOLDERS.—

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

(B) ANNUAL CERTIFICATION.—

(i) IN GENERAL.—Beginning 1 year after the date of 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 subparagraph (A) shall annually certify to the Commission, in a manner specified by the Commission, that the large data holder maintains—

(I) internal controls reasonably designed to comply with this Act; and

(II) internal reporting structures (as described in subparagraph (C)) to ensure that such certifying officers are involved in, and responsible for, decisions that impact compliance by the large data holder with this Act.

(ii) REQUIREMENTS.—A certification submitted under clause (i) shall be based on a review of the effectiveness of a large data holder's internal controls and reporting structures that is conducted by the certifying officers not more than 90 days before the submission of the certification.

(C) INTERNAL REPORTING STRUCTURE REQUIREMENTS.—At least 1 of the officers described in subparagraph (A) shall, either directly or through a supervised designee—

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

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

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

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

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

(D) PRIVACY IMPACT ASSESSMENTS.—

(i) IN GENERAL.—Not later than 1 year after the date of enactment of this Act or 1 year after the date that an entity first meets the definition of 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 entity's covered data collection, processing, retention, and transfer practices against the potential adverse consequences of such practices to individual privacy.

(ii) ASSESSMENT REQUIREMENTS.—A privacy impact assessment required under clause (i) shall be—

(I) reasonable and appropriate in scope given—

(aa) the nature and volume of the covered data collected, processed, retained, or transferred by the large data holder; and

(bb) 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, unless rendered out of date by a subsequent assessment conducted under clause (i); and

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

(iii) ADDITIONAL FACTORS TO INCLUDE IN ASSESSMENT.—In assessing the privacy risks, the large data holder shall include reviews of the means by which emerging technologies, including blockchain, distributed ledger technologies, privacy enhancing technologies, and other emerging technologies are used to secure covered data.

SEC. 11. SERVICE PROVIDERS AND THIRD PARTIES.

(a) Service Providers.—

(1) IN GENERAL.—A service provider—

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

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

(C) shall assist a covered entity in fulfilling the covered entity's obligations to respond to consumer rights requests pursuant to sections 5, 6, and 14 by appropriate

technical and organizational measures, taking into account the nature of the processing and the information reasonably available to the service provider;

(D) shall, upon the reasonable request of the covered entity, make available to the covered entity information necessary to demonstrate the service provider's compliance with the requirements of this Act;

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

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

(G) shall develop, implement, and maintain reasonable administrative, technical, and physical safeguards that are designed to protect the security and confidentiality of covered data the service provider processes consistent with section 9; and

(H) shall—

(i) allow and cooperate with reasonable assessments by the covered entity; or

(ii) arrange for a qualified and independent assessor to conduct an assessment of the service provider's policies and technical and organizational measures in support of the obligations under this Act, 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.

(2) CONTRACT REQUIREMENTS.—A contract between a covered entity and a service provider—

(A) shall govern the service provider's data processing procedures 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) shall not relieve a covered entity or service provider of any obligation under this Act; 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 service provider data with covered data which the service provider receives from or on behalf of another entity or collects from the interaction of the service provider with an individual, provided that such combining is not necessary to effectuate a purpose described in section 3(d) and is otherwise permitted under the contract required by this subsection.

(b) Third Parties.—A third party—

(1) shall not process, retain, or transfer third-party data for a purpose other than—

(A) in the case of sensitive covered data, the purpose for which an individual gave affirmative express consent for the transfer of the individual's sensitive covered data; 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 4;

(2) for purposes of paragraph (1), may reasonably rely on representations made by the covered entity that transferred the third-party data regarding the expectations of a reasonable person based on disclosures by the covered entity about the treatment of such data, provided that the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible; and

(3) shall be exempt from the requirements of section 3(b) with respect to third-party data, but shall otherwise have the same responsibilities and obligations as a covered entity with respect to such data under all other provisions of this Act.

(c) Rules of Construction.—

(1) SUCCESSIVE ACTOR VIOLATIONS.—

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

(B) KNOWLEDGE OF VIOLATION.—An entity 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 Act 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 Act shall not be in violation of this Act 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) Due Diligence.—

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

(2) TRANSFER TO THIRD PARTY.—A covered entity shall exercise reasonable due diligence in deciding to transfer covered data to a third party.

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

SEC. 12. DATA BROKERS.

(a) Notice.—A data broker shall—

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

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

(A) the entity is a data broker, using specific language that the Commission shall develop through guidance not later than 180 days after the date of enactment of this Act;

(B) an individual has a right to exercise the rights described in sections 5 and 6, including a link or other tool to allow an individual to exercise such rights;

(C) includes a link to the website established under subsection (c)(3); and

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

(b) Prohibited Practices.—A data broker is prohibited from—

(1) advertising or marketing the access to or transfer of covered data for the purposes of—

(A) stalking or harassing another individual; or

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

(2) misrepresenting 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 physical, email, and internet addresses of the data broker.

(ii) A description of the categories of covered data the data broker collects,

processes, retains, and transfers.

(iii) The contact information of the data broker, including the name of a contact person, a monitored telephone number, a 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 subsection (a)(2)(B).

(3) DATA BROKER REGISTRY.—

(A) ESTABLISHMENT.—The Commission shall establish and maintain on a publicly available website a searchable registry 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; and

(iii) includes a mechanism by which an individual may submit a request to all registered data brokers that are not consumer reporting agencies (as defined in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f))), and to the extent such third-party collecting entities are not acting as consumer reporting agencies (as so defined), a "Do Not Collect" directive such that any registered data broker shall ensure that the data broker no longer collects covered data related to such individual without the affirmative express consent of such individual, except insofar as the data broker is acting as a service provider.

(4) DO NOT COLLECT REQUESTS.—

(A) COMPLIANCE.—Subject to subparagraph (B), each data broker that receives a request from an individual using the mechanism established under paragraph (3)(B)(iii) shall comply with such request not later than 30 days after receiving such request.

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

(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 Congressionally designated entity that serves as the nonprofit national resource center and clearinghouse to provide assistance to victims, families, child-serving professionals, and the general public regarding issues related to missing and exploited children.

(d) Penalties.—

(1) IN GENERAL.—Subject to paragraph (2), a data broker that violates this section shall be liable for civil penalties as set forth in subsections (l) and (m) of section 5 of the Federal

Trade Commission Act, (15 U.S.C. 45(l), (m)).

(2) EXCEPTIONS.—A data broker that—

(A) fails to register with the Commission as required by subsection (c) shall be liable for—

(i) a civil penalty of $100 for each day the data broker fails to register, not to exceed a total of $10,000 for any year; and

(ii) an amount equal to the registration fee due under subsection (c)(2)(A) for each year that the data broker failed to register as required under subsection (c)(1); or

(B) fails to provide notice as required by subsection (a) shall be liable for a civil penalty of $100 for each day the data broker fails to provide such notice, not to exceed a total of $10,000 for any year.

(3) RULE OF CONSTRUCTION.—Except as set forth in paragraph (2), nothing in this subsection shall be construed as altering, limiting, or affecting any enforcement authority or remedy provided under this Act.

SEC. 13. CIVIL RIGHTS AND ALGORITHMS.

(a) Civil Rights Protections.—

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

(2) EXCEPTIONS.—This subsection shall not apply to—

(A) the collection, processing, retention, or transfer of covered data for the purpose of—

(i) a covered entity's or a service provider's self-testing to prevent or mitigate unlawful discrimination; or

(ii) diversifying an applicant, participant, or customer pool;

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

(C) advertising, marketing, or soliciting economic opportunities or benefits to underrepresented populations or members of protected classes as described in paragraph (1).

(b) FTC Enforcement Assistance.—

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

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

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

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

(3) TECHNICAL ASSISTANCE.—In transmitting information under paragraph (1), the Commission may consult and coordinate with, and provide technical and investigative assistance, as appropriate, to such Executive agency.

(4) COOPERATION WITH OTHER AGENCIES.—The Commission may implement this subsection by executing agreements or memoranda of understanding with the appropriate Executive agencies.

(c) Covered Algorithm Impact and Evaluation.—

(1) COVERED ALGORITHM IMPACT ASSESSMENT.—

(A) IMPACT ASSESSMENT.—Notwithstanding any other provision of law, not later than 2 years after the date of enactment of this Act, and annually thereafter, a large data holder that uses a covered algorithm in a manner that poses a consequential risk of a harm identified under subparagraph (B)(vi) to an individual or group of individuals and uses such covered algorithm, solely or in part, to collect, process, or transfer covered data shall conduct an impact assessment of such algorithm in accordance with subparagraph (B).

(B) IMPACT ASSESSMENT SCOPE.—The impact assessment required under subparagraph (A) shall provide the following:

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

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

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

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

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

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

(I) covered minors;

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

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

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

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

(2) ALGORITHM DESIGN EVALUATION.—Notwithstanding any other provision of law, not later than 2 years after the date of enactment of this Act, a covered entity or service provider that knowingly develops a covered algorithm shall, prior to deploying the covered algorithm in interstate commerce, evaluate the design, structure, and inputs of the covered algorithm, including any training data used to develop the covered algorithm, to reduce the risk of the potential harms identified under paragraph (1)(B)(vi).

(3) OTHER CONSIDERATIONS.—

(A) FOCUS.—In complying with paragraphs (1) and (2), a covered entity and a service provider may focus the impact assessment or evaluation on any covered algorithm, or portions of a covered algorithm, that will be put to use and may reasonably contribute to the risk of the potential harms identified under paragraph (1)(B)(vi).

(B) AVAILABILITY.—

(i) IN GENERAL.—A covered entity and a service provider—

(I) shall, not later than 30 days after completing an impact assessment or evaluation under paragraph (1) or (2), submit the impact assessment or evaluation to the Commission;

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

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

(ii) TRADE SECRETS.—A covered entity or service provider may redact and segregate any trade secret (as defined in section 1839 of title 18, United States Code) or other confidential or proprietary information from public disclosure under this subparagraph, and the Commission shall abide by its obligations under section 6(f) of the Federal Trade Commission Act (15 U.S.C. 46(f)) with respect to such information.

(C) LIMITATION ON ENFORCEMENT.—

(i) IN GENERAL.—Subject to clause (ii), the Commission may not use any information obtained solely and exclusively through a covered entity or a service provider's disclosure of information to the Commission in compliance with this section for any purpose other than to carry out the provisions of this Act, including the study and report described in paragraph (6).

(ii) EXCEPTIONS.—

(I) PROVISION TO CONGRESS.—The limitation described in clause (i) does not preclude the Commission from providing such information to Congress in response to a subpoena.

(II) CONSENT ORDERS.—The limitation described in clause (i) does not preclude the Commission from enforcing a consent order entered into with the applicable covered entity or service provider.

(4) GUIDANCE.—Not later than 2 years after the date of enactment of this Act, the Commission shall, in consultation with the Secretary of Commerce, publish guidance regarding compliance with this section.

(5) RULEMAKING AND EXEMPTION.—The Commission may promulgate regulations, in accordance with section 553 of title 5, United States Code, as necessary to establish processes by which a—

(A) large data holder shall submit an impact assessment to the Commission under paragraph (3)(B)(i)(I); and

(B) large data holder, covered entity, or service provider may exclude from this subsection any covered algorithm that presents low or minimal risk of the potential harms identified under paragraph (1)(B)(vi) to an individual or group of individuals.

(6) STUDY AND REPORT.—

(A) STUDY.—The Commission, in consultation with the Secretary of Commerce, shall conduct a study, to review any impact assessment or evaluation submitted under this subsection. Such study shall include an examination of—

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

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

(B) REPORT.—

(i) INITIAL REPORT.—Not later than 3 years after the date of enactment of this Act, the Commission, in consultation with the Secretary of Commerce, shall submit to Congress a report containing the results of the study conducted under subparagraph (A), together with recommendations for such legislation and administrative action as the Commission determines appropriate.

(ii) ADDITIONAL REPORTS.—Not later than 3 years after submission of the initial report under clause (i), and as the Commission determines necessary thereafter, the Commission shall submit to Congress an updated version of such report.

SEC. 14. CONSEQUENTIAL DECISION OPT OUT.

(a) In General.—An entity that uses a covered algorithm to make or facilitate a consequential decision shall—

(1) provide—

(A) notice to any individual subject to such use of the covered algorithm; and

(B) an opportunity for the individual to opt out of such use of the covered algorithm; and

(2) abide by any opt-out designation made by an individual under paragraph (1)(B).

(b) Notice.—The notice required under subsection (a)(1)(A) shall—

(1) be clear, conspicuous, and not misleading;

(2) provide meaningful information about how the covered algorithm makes or facilitates a consequential decision, including the range of potential outcomes;

(3) be provided in each language in which the entity—

(A) provides a product or service subject to the use of such covered algorithm; or

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

(4) be reasonably accessible to and usable by individuals with disabilities.

(c) Guidance.—Not later than 2 years after the date of enactment of this Act, the Commission, in consultation with the Secretary of Commerce, shall publish guidance regarding compliance with this section.

(d) Consequential Decision Defined.—For the purposes of this section, the term "consequential decision" means a determination or an offer, including through advertisement, that uses covered data and relates to—

(1) an individual's or a class of individuals' access to or equal enjoyment of housing, employment, education enrollment or opportunity, healthcare, insurance, or credit opportunities; or

(2) access to, or restrictions on the use of, any place of public accommodation.

SEC. 15. 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, may apply to the Commission for approval of 1 or more sets of compliance guidelines governing the collection, processing, retention, and transfer of covered data by the covered entity.

(2) APPLICATION REQUIREMENTS.—Such application shall include—

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

(B) a description of the entities or activities the proposed set of compliance guidelines is 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 compliance guidelines;

(D) a description of the independent organization, which shall not be associated with any of the participating covered entities, that will administer the compliance guidelines; and

(E) and a description of how such entities will be assessed for adherence to such compliance 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 receiving an application under paragraph (1), the Commission shall publish the application and provide an opportunity for public comment on the compliance guidelines proposed in such application.

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

(I) meet or exceed requirements of this Act;

(II) will provide for the regular review and validation by the independent organization to ensure that the covered entity continues to meet or exceed the requirements of this Act; and

(III) include a means of enforcement if a covered entity does not meet or exceed the requirements in the guidelines, which may include referral to the Commission for enforcement consistent with section 17 or referral to the appropriate State attorney general for enforcement consistent with section 18.

(iii) TIMELINE.—Not later than 1 year after receiving an application under paragraph (1), the Commission shall issue a determination approving or denying the application, including the independent organization the application proposed to administer the compliance guidelines proposed in such application, and providing an explanation for such approval or denial.

(B) APPROVAL OF MODIFICATIONS.—

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

(ii) TIMELINE.—Not later than 1 year after receiving the updated compliance guidelines under clause (i), the Commission shall issue a determination approving or denying the material change to such guidelines.

(b) Withdrawal of Approval.—

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

(2) OPPORTUNITY TO CURE.—

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

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

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

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

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

(d) Rebuttable Presumption of Compliance.—A covered entity with compliance guidelines approved by the Commission under this section, and that is in compliance with such guidelines, shall be entitled to a rebuttable presumption that such entity is in compliance with the relevant provisions of this Act if such covered entity is in compliance with such guidelines.

SEC. 16. PRIVACY-ENHANCING TECHNOLOGY PILOT PROGRAM.

(a) In General.—Not later than 1 year after the date of enactment of this Act, the Commission shall establish and carry out a pilot program to encourage private sector use of privacy-enhancing technology for the purpose of protecting covered data in compliance with section 9.

(b) Covered Entity Participation.—

(1) APPLICATION PROCESS.—A covered entity seeking to participate in the pilot program established under subsection (a) shall submit to the Commission, in such time, form, and manner as the Commission may require, an application that demonstrates the ability of the covered entity to use privacy-enhancing technology to establish data security practices that meet or exceed the requirements of section 9.

(2) LIMITATIONS ON LIABILITY.—Any covered entity selected by the Commission to participate in the pilot program shall—

(A) with respect to any action under section 17 or 18 for a violation of section 9, be

deemed to be in compliance with section 9 with respect to any covered data subject to the privacy-enhancing technology; and

(B) for any action under section 19 alleging a data breach due to a violation of section 9, be entitled to a rebuttable presumption that such covered entity is in compliance with the relevant requirements under section 9 with respect to any covered data subject to the privacy-enhancing technology.

(3) AUDIT OF COVERED ENTITIES.—

(A) IN GENERAL.—The Commission shall, on an ongoing basis, audit each covered entity participating in the pilot program to determine whether the covered entity is maintaining the use and implementation of privacy-enhancing technology to secure covered data.

(B) REMOVAL.—

(i) IN GENERAL.—If at any time the Commission determines that a covered entity participating in the pilot program is no longer maintaining the use and implementation of privacy-enhancing technology, the Commission shall—

(I) notify the covered entity of such determination; and

(II) subject to clause (ii), remove such covered entity from participation in the pilot program, including the limitations on liability described in paragraph (2) that are afforded to participants.

(ii) OPPORTUNITY TO CURE.—Not later than 180 days after receiving notice from the Commission under clause (i), a covered entity may cure any alleged deficiency with its use and implementation of privacy-enhancing technology and submit to the Commission such proposed cure. If the Commission determines that such cure eliminates the alleged deficiency, then the Commission may not remove the covered entity from participation in the pilot program.

(c) Coordination.—In carrying out the pilot program under subsection (a), the Commission shall—

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

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

(d) GAO Study and Report.—

(1) STUDY.—Not later than 3 years after the date of enactment of this Act, the Comptroller General of the United States (in this subsection referred to as the "Comptroller General") shall conduct a study to—

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

(B) evaluate the Commission's use of privacy-enhancing technology to support oversight of covered entities' data security practices; and

(C) develop recommendations to improve and advance privacy-enhancing

technology, including by improving communication and coordination between covered entities and the Commission to increase use and implementation of privacy-enhancing technology by such entities and the Commission.

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

(3) FINAL REPORT.—Not later than 240 days after the initial briefing under paragraph (2), the Comptroller General 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 final report describing the results of the study conducted under paragraph (1), including the recommendations developed under subparagraph (C) of such paragraph.

(e) Sunset.—The Commission shall terminate the pilot program established under subsection (a) not later than 10 years after the date on which the pilot program is established.

(f) Privacy-enhancing Technology Defined.—The term "privacy-enhancing technology"—

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

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

SEC. 17. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) New Bureau.—

(1) IN GENERAL.—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 Commission's authority under this Act and related authorities.

(3) TIMELINE.—The bureau shall be established, staffed, and fully operational not later than 1 year after the date of enactment of this Act.

(b) Enforcement by the Federal Trade Commission.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act, or a regulation promulgated under this Act, 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 THE COMMISSION.—

(A) IN GENERAL.—Except as provided in paragraphs (3) and (4) or otherwise

provided in this Act, the Commission shall enforce this Act and the regulations promulgated under this Act 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 Act.

(B) PRIVILEGES AND IMMUNITIES.—Any entity that violates this Act or a regulation promulgated under this Act 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 Act and the regulations promulgated under this Act in the same manner provided in paragraphs (1) and (2), with respect to—

(A) common carriers subject to title II of the Communications Act of 1934 (47 U.S.C. 201–231) as currently enacted or subsequently amended; an

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

(4) PRIVACY AND SECURITY VICTIMS RELIEF FUND.—

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

(B) DEPOSITS.—

(i) DEPOSITS FROM THE COMMISSION.—The Commission shall deposit into the Victims Relief Fund the amount of any civil penalty obtained against any entity in any judicial or administrative action the Commission commences to enforce this Act or a regulation promulgated under this Act.

(ii) DEPOSITS FROM THE ATTORNEY GENERAL OF THE UNITED STATES.—The Attorney General of the United States shall deposit into the Victims Relief Fund the amount of any civil penalty obtained against any entity in any judicial or administrative action the Attorney General commences on behalf of the Commission to enforce this Act or a regulation promulgated under this Act.

(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, payments or compensation, or other monetary relief to persons affected by an act or practice for which civil penalties have been obtained under this Act.

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

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

(II) engaging in technological research that the Commission considers necessary to enforce this Act.

(D) CALCULATION.—

(i) PENALTY OFFSET FOR STATE OR INDIVIDUAL ACTIONS.—Any amount that a court orders an entity to pay under this subsection shall be offset by any amount the person received from an action brought against the entity for the same violation under section 18 or 19.

(ii) RELIEF OFFSET FOR STATE OR INDIVIDUAL ACTIONS.—Any amount that the Commission provides to a person as redress, payments or compensation, or other monetary relief under subparagraph (C) shall be offset by any amount the person received from an action brought against the entity for the same violation under section 18 or 19.

(E) RULE OF CONSTRUCTION.—Amounts collected and deposited in the Victims Relief Fund shall not be construed to be government funds or appropriated monies and shall 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 on investigations conducted for alleged violations this Act, including—

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

(B) the number of such investigations the Commission has 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.—The report required under paragraph (1) shall not include the identity of the person who is the subject of the investigation or any other information that identifies such 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 Act, including each of the following:

(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 guidance required under this Act.

(D) Any plans to restructure the Commission or establish, alter, or terminate working groups.

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

SEC. 18. 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 the 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 that State has been or is adversely affected by the engagement of any entity in an act or practice that violates this Act or a regulation promulgated under this Act, the attorney general, chief consumer protection officer, or other authorized officer 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 that act or practice;

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

(C) obtain civil penalties;

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

(E) obtain reasonable attorneys' 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 where the attorney general of a State, the chief consumer protection officer of a State, or an officer of office of the 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 of the same State may institute a civil action under paragraph (1) against the same defendant for the same violation of this Act or a regulation promulgated under this Act.

(b) Rights of the Commission.—

(1) IN GENERAL.—Except where not feasible, the 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.—Where it is not feasible for the 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 Act or a regulation promulgated under this Act, no attorney general of a State, chief consumer protection officer of a State, or officer or office of the 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 Act or a regulation promulgated under this Act that is alleged in such complaint.

(d) Investigatory Powers.—Nothing in this section shall 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 the 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 Federal district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

(f) GAO Study.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall conduct a study on State attorneys general's hiring of, or otherwise contracting with, outside firms to assist in the enforcement of this Act. The study shall include—

(1) the frequency of such hires;

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

(3) the types of matters outside firms are hired or contracted with for;

(4) the bid process for such outside law firm work and selection process, including reviews of conflicts of interest;

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

(6) the percent of monetary recovery that is returned to victims and the percent that is retained by the law firm; and

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

(g) Calculation.—Any amount that a court orders an entity to pay in an action brought under subsection (a) shall be offset by any amount the person received from an action brought against the entity for the same violation under section 17 or 19.

(h) Preservation of State Powers.—Except as provided in subsection (c), no provision of this

section shall 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 that State; or

(2) exercise the powers conferred on the attorney general, the chief consumer protection officer of a State, or such officer or office by the laws of the 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.

SEC. 19. ENFORCEMENT BY INDIVIDUALS.

(a) Enforcement by Individuals.—

(1) IN GENERAL.—Subject to subsections (b) and (c), an individual may bring a civil action against an entity for a violation of subsections (b) or (c) of section 3, subsections (a) or (e) of section 4, section 5, subsections (a) or (b)(2) of section 6, section 7, section 8, section 9 to the extent such claim alleges a data breach arising from a violation of subsection (a) of such section, subsection (d) of section 11, subsection (c)(4) of section 12, subsection (a) of section 13, section 14, 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 the entity retrieve any covered data transferred in violation of this Act;

(iii) declaratory relief; and

(iv) reasonable attorney's fees and litigation costs.

(B) BIOMETRIC AND GENETIC INFORMATION.—In a civil action brought under paragraph (1) for a violation of this Act with respect to section 3(c) where the conduct underlying the violation occurred primarily and substantially in Illinois, in which the plaintiff prevails, the court may award the plaintiff—

(i) the same relief as set forth in section 20 of the Biometric Information Privacy Act (740 ILCS 14/20), as such statute read on January 1, 2024; or

(ii) the same relief as set forth in section 40 of the Genetic Information Privacy Act (740 ILCS 513/40), as such statute read on January 1, 2024.

(C) DATA SECURITY.—

(i) IN GENERAL.—In a civil action brought under paragraph (1) for a violation of section 9, alleging unauthorized access of covered information (as defined in clause (ii)) 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—

(I) an individual's username, email address, or telephone number 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; or

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

(aa) A government identifier as described in section 2(34)(A)(i).

(bb) Any sensitive covered data described in section 2(34)(A)(iv).

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

(dd) Biometric information.

(ee) Genetic information.

(D) LIMITATIONS ON DUAL ACTIONS.—Any amount that a court orders an entity to pay to an individual under subparagraph (A)(i), (B), or (C) shall be offset by any amount the individual received from an action brought against the entity for the same violation under section 17 or 18.

(b) Opportunity to Cure in Actions for Injunctive Relief.—

(1) NOTICE.—Subject to paragraph (3), an action for injunctive relief may be brought by an individual under this section only if, prior to initiating such action against an entity, the individual provides to the entity 30 days' written notice identifying the specific provisions of this Act the individual alleges have been or are being violated.

(2) EFFECT OF CURE.—In the event a cure is possible, if, within the 30-day period, the entity cures the noticed violation and provides the individual with an express written statement that the violation has been cured and that no such further violation shall occur, an action for injunctive relief shall not be permitted.

(3) SUBSTANTIAL PRIVACY HARM.—Notice shall not be required under paragraph (1) prior to filing an action for injunctive relief for a violation of this Act that resulted in a substantial privacy harm.

(c) Notice of Actions Seeking Actual Damages.—

(1) NOTICE.—Subject to paragraph (2), an action for actual damages may be brought by an individual under this section only if, prior to initiating such action against an entity, the individuals provides to the entity 30 days' written notice identifying the specific provisions of this Act the individual alleges have been or are being violated.

(2) SUBSTANTIAL PRIVACY HARM.—Notice shall not be required under paragraph (1) prior

to filing an action for actual damages for a violation of this Act that resulted in a substantial privacy harm if such action includes a claim for a preliminary injunction or temporary restraining order.

(d) Predispute Arbitration Agreements.—

(1) IN GENERAL.—Notwithstanding any other provision of law, at the election of the individual alleging a violation of this Act, 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 section applies to a dispute shall be determined under Federal law. The applicability of this section to an agreement to arbitrate and the validity and enforceability of an agreement to which this section 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 such agreement, and irrespective of whether the agreement purports to delegate such determination to an arbitrator.

(3) DEFINITION OF PREDISPUTE ARBITRATION AGREEMENT.—For purposes of this subsection, the term "predispute arbitration agreement" means any agreement to arbitrate a dispute that has not arisen at the time of the making of the agreement.

(e) Clarification.—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 subsection.

SEC. 20. RELATION TO OTHER LAWS.

(a) Preemption of State Laws.—

(1) PURPOSES.—The purposes of this Act are to—

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

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

(2) IN GENERAL.—Except as provided in paragraph (3), no State or political subdivision thereof may adopt, maintain, enforce, or continue in effect any law, regulation, rule, or requirement covered by the provisions of this Act or a rule, regulation, or requirement promulgated under this Act.

(3) STATE LAW PRESERVATION.—Paragraph (1) shall 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) Provision of laws that address notification requirements in the event of a data breach.

(F) Contract or tort law.

(G) Criminal laws unrelated to data privacy or data security.

(H) Criminal or civil laws regarding—

(i) blackmail;

(ii) stalking, including cyberstalking;

(iii) cyberbullying;

(iv) intimate images, including authentic or generated by a computer or by artificial intelligence, 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 data privacy or data security, provided that such laws do not directly conflict with the provisions of this Act.

(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, telephone monitoring.

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

(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.

(b) Federal Law Preservation.—

(1) IN GENERAL.—Nothing in this Act or a regulation promulgated under this Act 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 Act.

(2) ANTITRUST SAVINGS CLAUSE.—

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

(i) has the meaning given that 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 that section applies to unfair methods of competition.

(B) RULE OF CONSTRUCTION.—Nothing in this Act, or the regulatory regime created under this Act, may be construed to modify, impair, supersede the operation of, or preclude the application of the antitrust laws.

(3) APPLICATION OF OTHER FEDERAL PRIVACY REQUIREMENTS.—

(A) IN GENERAL.—A covered entity or service provider that is required to comply with the laws and regulations described in subparagraph (B) and is in compliance with the data privacy requirements of such laws and regulations shall be deemed to be in compliance with the related provisions of this Act (except with respect to section 9), solely and exclusively with respect to any data subject to the requirements of such laws and regulations.

(B) LAWS AND REGULATIONS DESCRIBED.—For purposes of subparagraph (A), the 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. 17931 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 thereunder.

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

(vii) Section 444 of the General Education Provisions Act of 1974 (commonly known as the "Family Educational Rights and Privacy Act") (20 U.S.C. 1232g) and part 99 of title 34, Code of Federal Regulations (or any successor regulation),

to the extent such covered entity or service provider is an educational agency or institution as defined in such section of such Act or section 99.3 of title 34, Code of Federal Regulations (or any successor regulation).

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

(4) APPLICATION OF OTHER FEDERAL DATA SECURITY REQUIREMENTS.—

(A) IN GENERAL.—A covered entity or service provider that is required to comply with the laws and regulations described in subparagraph (B) and is in compliance with the information security requirements of such laws and regulations shall be deemed to be in compliance with section 9 of this Act, solely and exclusively with respect to any data subject to the requirements of such laws and regulations.

(B) LAWS AND REGULATIONS DESCRIBED.—For purposes of subparagraph (A), the 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) The Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.).

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

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

(c) Preservation of Common Law or Statutory Causes of Action for Civil Relief.—Nothing in this Act nor any amendment, standard, rule, requirement, assessment, law, or regulation promulgated under this Act shall be construed to preempt, displace, or supplant any Federal or State common law right or remedy, or any 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, or an objectively offensive intrusion into the private affairs or concerns of the individual, or any other legal theory of liability under any Federal or State common law, or any State statutory law, except that a violation of this Act or a regulation promulgated under this Act may not be pleaded as an element of any violation of such law.

(d) Non-application of Certain Provisions of the Communications Act of 1934.—

(1) IN GENERAL.—Notwithstanding any other provision of law, and except as provided in paragraph (2), the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof or supplementary thereto and any regulation promulgated by the Federal Communications Commission under such an Act shall not apply to any covered entity or service provider with respect to the collection, processing, retention, transfer, or security of covered data to the extent that such collection, processing, retention, transfer, or security of covered data is governed by the requirements of this Act.

(2) EXCEPTIONS.—Paragraph (1) shall not preclude the application of any of the following to a covered entity or service provider with respect to the collection, processing, retention, transfer, or security of covered data:

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

(B) Section 64.2011 of title 47, Code of Federal Regulations (or any successor regulation).

(C) Mitigation measures and actions taken pursuant to Executive Order 13913 (85 Fed. Reg. 19643; relating to the establishment of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector).

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

SEC. 21. CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998.

Nothing in this Act 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. 22. TERMINATION OF FTC RULEMAKING ON COMMERCIAL SURVEILLANCE AND DATA SECURITY.

Beginning on the date of enactment of this Act, the Commission's Trade Regulation Rule on Commercial Surveillance and Data Security proposed rulemaking, as published on August, 8, 2022, shall be terminated.

SEC. 23. SEVERABILITY.

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

SEC. 24. EFFECTIVE DATE.

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