117TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
117–669

AMERICAN DATA PRIVACY AND PROTECTION ACT

DECEMBER 30, 2022.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. PALLONE, from the Committee on Energy and Commerce, submitted the following

R E P O R T

[To accompany H.R. 8152]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 8152) to provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "American Data Privacy and Protection Act".

(b) TABLE OF CONTENTS.—The table of contents of 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 clearly communicates the individual's freely given, specific, and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a covered entity that meets the requirements of subparagraph (B).

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

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

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

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

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

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

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

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

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

(vii) Processing or transferring any covered data collected pursuant to affirmative express consent for a different processing purpose than

that for which affirmative express consent was obtained shall require affirmative express consent for the subsequent processing purpose.

(C) EXPRESS CONSENT REQUIRED.—A covered entity may not infer that an individual has provided affirmative express consent to an act or practice from the inaction of the individual or the individual's continued use of a service or product provided by the covered entity.

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

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

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

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

(3) BIOMETRIC INFORMATION.—

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

(i) fingerprints;

(ii) voice prints;

(iii) iris or retina scans;

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

(v) gait or personally identifying physical movements.

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

(i) a digital or physical photograph;

(ii) an audio or video recording; or

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

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

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

(6) 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.

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

(8) COVERED DATA.—

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

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

(i) de-identified data;

(ii) employee data;

(iii) publicly available information; or

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

(C) EMPLOYEE DATA DEFINED.—For purposes of subparagraph (B), the term "employee data" means—

(i) information relating to a job applicant collected by a covered entity acting as a prospective employer of such job applicant in the course of the application, or hiring process, if such information is collected, proc-

essed, or transferred by the prospective employer solely for purposes related to the employee's status as a current or former job applicant of such employer;

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

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

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

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

(9) COVERED ENTITY.—

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

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

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

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

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

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

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

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

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

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

(C) NON-APPLICATION TO SERVICE PROVIDERS.—An entity shall not be considered to be a covered entity for purposes of this Act in so far as the entity is acting as a service provider (as defined in paragraph (29)).

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

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

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

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

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

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

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

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

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

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

(13) 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.

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

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

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

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

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

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

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

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

(20) KNOWLEDGE.—

(A) IN GENERAL.—The term "knowledge" means—

(i) with respect to a covered entity that is a covered high-impact social media company, the entity knew or should have known the individual was a covered minor;

(ii) with respect to a covered entity or service provider that is a large data holder, and otherwise is not a covered high-impact social media company, that the covered entity knew or acted in willful disregard of the fact that the individual was a covered minor; and

(iii) with respect to a covered entity or service provider that does not meet the requirements of clause (i) or (ii), actual knowledge.

(B) COVERED HIGH-IMPACT SOCIAL MEDIA COMPANY.—For purposes of this paragraph, the term "covered high-impact social media company" means a covered entity that provides any internet-accessible platform where—

(i) such covered entity generates $3,000,000,000 or more in annual revenue;

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

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

(21) LARGE DATA HOLDER.—

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

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

(ii) collected, processed, or transferred—

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

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

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

(i) personal email addresses;

(ii) personal telephone numbers; or

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

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

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

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

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

(A) integrated into any product or service;

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

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

(23) MATERIAL.—The term "material" means, with respect to an act, practice, or representation of a covered entity (including a representation made by the covered entity in a privacy policy or similar disclosure to individuals) involving the collection, processing, or transfer of covered data, that such act, practice, or representation is likely to affect a reasonable individual's decision or conduct regarding a product or service.

(24) PRECISE GEOLOCATION INFORMATION.—

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

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

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

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

(27) PUBLICLY AVAILABLE INFORMATION.—

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

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

(ii) widely distributed media;

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

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

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

(B) CLARIFICATIONS; LIMITATIONS.—

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

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

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

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

(III) biometric information;

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

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

(VI) intimate images known to be nonconsensual.

(28) SENSITIVE COVERED DATA.—

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

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

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

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

(iv) Biometric information.

(v) Genetic information.

(vi) Precise geolocation information.

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

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

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

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

vided by an employer to an employee insofar as such employer provides conspicuous notice that it may access such information.

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

(xii) Information revealing the video content requested or selected by an individual collected by a covered entity that is not a provider of a service described in section 102(4). This clause does not include covered data used solely for transfers for independent video measurement.

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

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

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

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

(B) RULEMAKING.—The Commission may commence a rulemaking pursuant to section 553 of title 5, United States Code, to include in the definition of "sensitive covered data" any other type of covered data that may require a similar level of protection as the types of covered data listed in clauses (i) through (xvi) of subparagraph (A) as a result of any new method of collecting, processing, or transferring covered data.

(29) SERVICE PROVIDER.—

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

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

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

(B) TREATMENT WITH RESPECT TO SERVICE PROVIDER DATA.—A service provider that receives service provider data from another service provider as permitted under this Act shall be treated as a service provider under this Act with respect to such data.

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

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

(32) STATE PRIVACY AUTHORITY.—The term "State privacy authority" means—

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

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

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

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

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

(B) does not include—

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

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

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

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

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

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

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

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

(36) THIRD-PARTY COLLECTING ENTITY.—

(A) IN GENERAL.—The term "third-party collecting entity"—

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

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

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

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

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

(C) NON-APPLICATION TO SERVICE PROVIDERS.—An entity may not be considered to be a third-party collecting entity for purposes of this Act if the entity is acting as a service provider.

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

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

(39) UNIQUE PERSISTENT IDENTIFIER.—The term "unique identifier"—

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

(B) does not include an identifier assigned by a covered entity for the specific purpose of giving effect to an individual's exercise of affirmative express consent or opt-outs of the collection, processing, and transfer of covered data pursuant to section 204 or otherwise limiting the collection, processing, or transfer of such information.

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

TITLE I—DUTY OF LOYALTY

SEC. 101. DATA MINIMIZATION.

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

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

(2) effect a purpose permitted under subsection (b).

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

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

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

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

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

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

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

(E) to protect against spam; or

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

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

(4) To fulfill a product or service warranty.

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

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

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

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

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

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

(i) is in the public interest; and

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

(B) Not later than 18 months after the date of enactment of this Act, the Commission should issue guidelines to help covered entities ensure the privacy of affected users and the security of covered data, particularly as data is being transferred to and stored by researchers. Such guidelines should consider risks as they pertain to projects using covered data with special considerations for projects that are exempt under part 46 of title 45, Code of Federal Regulations (or any successor regulation) or are excluded from the criteria for institutional review board review.

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

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

(13) 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 the entity or entities receiving the individual's covered data and their privacy policies as described in section 202; and

(B) a reasonable opportunity to withdraw any previously given consents in accordance with the requirements of affirmative express consent under this Act related to the individual's covered data and a reasonable opportunity to request the deletion of the individual's covered data, as described in section 203.

(14) To ensure the data security and integrity of covered data, as described in section 208.

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

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

(17) With respect to covered data previously collected in accordance with this Act, notwithstanding this exception and provided such collection, processing, and transferring otherwise complies with the requirements of this Act, including section 204(c), to provide targeted advertising.

(c) GUIDANCE.—The Commission shall issue guidance regarding what is reasonably necessary and proportionate to comply with this section. Such guidance shall take into consideration—

(1) the size of, and the nature, scope, and complexity of the activities engaged in by, the covered entity, including whether the covered entity is a large data holder, nonprofit organization, covered entity meeting the requirements of section 209, third party, or third-party collecting entity;

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

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

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

(d) DECEPTIVE MARKETING OF A PRODUCT OR SERVICE.—A covered entity or service provider may not engage in deceptive advertising or marketing with respect to a product or service offered to an individual.

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

SEC. 102. LOYALTY DUTIES.

Notwithstanding section 101 and unless an exception applies, with respect to covered data, a covered entity or service provider may not—

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

(2) collect or process sensitive covered data, except where such collection or processing is strictly necessary to provide or maintain a specific product or service requested by the individual to whom the covered data pertains, or is strictly necessary to effect a purpose enumerated in paragraphs (1) through (12) and (14) through (15) of section 101(b);

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

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

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

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

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

(E) in the case of the transfer of a password, the transfer is necessary to use a designated password manager or is to a covered entity for the ex-

clusive purpose of identifying passwords that are being re-used across sites or accounts;

(F) in the case of the transfer of genetic information, the transfer is necessary to perform a medical diagnosis or medical treatment specifically requested by an individual, or to conduct medical research in accordance with conditions of section 101(b)(10); or

(G) to transfer assets in the manner described in paragraph (13) of section 101(b); or

(4) in the case of a provider of broadcast television service, cable service, satellite service, streaming media service, or other video programming service described in section 713(h)(2) of the Communications Act of 1934 (47 U.S.C. 613(h)(2)), transfer to an unaffiliated third party covered data that reveals the video content or services requested or selected by an individual from such service, except with the affirmative express consent of the individual or pursuant to one of the permissible purposes enumerated in paragraphs (1) through (15) of section 101(b).

SEC. 103. PRIVACY BY DESIGN.

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

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

(2) identify, assess, and mitigate privacy risks related to covered minors (including, if applicable, with respect to a covered entity that is not an entity meeting the requirements of section 209, in a manner that considers the developmental needs of different age ranges of covered minors) to result in reasonably necessary and proportionate residual risk to covered minors;

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

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

(b) FACTORS TO CONSIDER.—The policies, practices, and procedures established by a covered entity and a service provider under subsection (a), shall correspond with, as applicable—

(1) the size of the covered entity or the service provider and the nature, scope, and complexity of the activities engaged in by the covered entity or service provider, including whether the covered entity or service provider is a large data holder, nonprofit organization, entity meeting the requirements of section 209, third party, or third-party collecting entity, taking into account the role of the covered entity or service provider and the information available to it;

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

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

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

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

(c) COMMISSION GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance as to what constitutes reasonable policies, practices, and procedures as required by this section. The Commission shall consider unique circumstances applicable to nonprofit organizations, to entities meeting the requirements of section 209, and to service providers.

SEC. 104. LOYALTY TO INDIVIDUALS WITH RESPECT TO PRICING.

(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 goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services.

(b) RULES OF CONSTRUCTION.—Nothing in subsection (a) may be construed to—

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

(2) prohibit a covered entity from offering a different price, rate, level, quality or selection of goods or services to an individual, including offering goods or services for no fee, if the offering is in connection with an individual's voluntary participation in a bona fide loyalty program;

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

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

(5) prohibit a covered entity from offering different types of pricing or functionalities with respect to a product or service based on an individual's exercise of a right under section 203(a)(3); or

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

(c) BONA FIDE LOYALTY PROGRAM DEFINED.—For purposes of this section, the term "bona fide loyalty program" includes rewards, premium features, discount or club card programs.

TITLE II—CONSUMER DATA RIGHTS

SEC. 201. CONSUMER AWARENESS.

(a) IN GENERAL.—Not later than 90 days after the date of enactment of this Act, the Commission shall publish, on the public website of the Commission, a webpage that describes each provision, right, obligation, and requirement of this Act, listed separately for individuals and for covered entities and service providers, and the remedies, exemptions, and protections associated with this Act, in plain and concise language and in an easy-to-understand manner.

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

(c) ACCESSIBILITY.—The Commission shall publish the information required to be published under subsection (a) in the ten languages with the most users in the United States, according to the most recent United States Census.

SEC. 202. TRANSPARENCY.

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

(b) CONTENT OF PRIVACY POLICY.—A covered entity or service provider shall have a privacy policy that includes, 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 covered entity's or service provider's points of contact and generic electronic mail addresses, as applicable for privacy and data security inquiries); and

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

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

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

(4) Whether the covered entity or service provider transfers covered data and, if so, each category of service provider and third party to which the covered entity or service provider transfers covered data, the name of each third-party collecting entity to which the covered entity or service provider transfers covered data, and the purposes for which such data is transferred to such categories of service providers and third parties or third-party collecting entities, except for a transfer to a governmental entity pursuant to a court order or law that prohibits the covered entity or service provider from disclosing such transfer, ex-

cept for transfers to governmental entities pursuant to a court order or law that prohibits the covered entity from disclosing the transfer.

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

(6) A prominent description of how an individual can exercise the rights described in this Act.

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

(8) The effective date of the privacy policy.

(9) Whether or not any covered data collected by the covered entity or service provider is transferred to, processed in, stored in, or otherwise accessible to the People's Republic of China, Russia, Iran, or North Korea.

(c) LANGUAGES.—The privacy policy required under subsection (a) shall be made available to the public in each covered 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 also provide the disclosures under this section in a manner that is reasonably accessible to and usable by individuals with disabilities.

(e) MATERIAL CHANGES.—

(1) AFFIRMATIVE EXPRESS CONSENT.—If a covered entity makes a material change to its privacy policy or practices, the covered entity shall notify each individual affected by such material change before implementing the material change with respect to any prospectively collected covered data and, except as provided in paragraphs (1) through (15) of section 101(b), provide a reasonable opportunity for each individual to withdraw consent to any further materially different collection, processing, or transfer of previously collected covered data under the changed policy.

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

(3) CLARIFICATION.—Nothing in this section may be construed to affect the requirements for covered entities under section 102 or 204.

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

(f) SHORT-FORM NOTICE TO CONSUMERS BY LARGE DATA HOLDERS.—

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

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

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

(C) inclusive of an overview of individual rights and disclosures to reasonably draw attention to data practices that may reasonably be unexpected to a reasonable person or that involve sensitive covered data; and

(D) no more than 500 words in length.

(2) RULEMAKING.—The Commission shall issue a rule pursuant to section 553 of title 5, United States Code, establishing the minimum data disclosures necessary for the short-form notice required under paragraph (1), which shall not exceed the content requirements in subsection (b) and shall include templates or models of short-form notices.

SEC. 203. INDIVIDUAL DATA OWNERSHIP AND CONTROL.

(a) ACCESS TO, AND CORRECTION, DELETION, AND PORTABILITY OF, COVERED DATA.—In accordance with subsections (b) and (c), a covered entity shall provide an individual, after receiving a verified request from the individual, with the right to—

(1) access—

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

(B) the categories of any third party, if applicable, and an option for consumers to obtain the names of any such third party as well as and the categories of any service providers to whom the covered entity has transferred for consideration 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 verifiable substantial inaccuracy or substantially incomplete information with respect to the covered data of the individual that is processed by the covered entity and instruct the covered entity to make reasonable efforts to notify all third parties or service providers to which the covered entity transferred such covered data of the corrected information;

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

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

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

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

(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 subsection (a) through—

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

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

(c) TIMING.—

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

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

(B) covered entity that is not a large data holder or a covered entity meeting the requirements of section 209 within 60 days of such request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual; or

(C) covered entity meeting the requirements of section 209 within 90 days of such request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual.

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

(d) FREQUENCY AND COST OF ACCESS.—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 2 times that an individual exercises any right described in subsection (a) in any 12-month period, shall allow the individual to exercise such right free of charge; and

(B) any time beyond the initial 2 times described in subparagraph (A), may allow the individual to exercise such right for a reasonable fee for each request.

(e) VERIFICATION AND EXCEPTIONS.—

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

(A) cannot reasonably verify that the individual making the request to exercise the right 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) reasonably believes that the request is made to interfere with a contract between the covered entity and another individual;

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

(D) reasonably believes that the exercise of the right would require the covered entity to engage in an unfair or deceptive practice under section 5 of the Federal Trade Commission Act (15 U.S.C. 45); or

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

(2) ADDITIONAL INFORMATION.—If a covered entity cannot reasonably verify that a request to exercise a right described in subsection (a) is made by the individual whose covered data is the subject of the request (or an individual authorized to make such a request on the individual's behalf), the covered entity—

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

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

(3) PERMISSIVE EXCEPTIONS.—

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

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

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

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

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

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

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

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

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

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

(x) fall within an exception enumerated in the regulations promulgated by the Commission pursuant to subparagraph (D); or

(xi) with respect to requests for deletion—

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

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

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

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

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

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

(B) PARTIAL COMPLIANCE.—In a circumstance that would allow a denial pursuant to subparagraph (A), a covered entity shall partially comply with the remainder of the request if it is possible and not unduly burdensome to do so.

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

(D) FURTHER EXCEPTIONS.—The Commission may, by regulation as described in subsection (g), 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. In establishing such exceptions, the Commission should consider any relevant changes in technology, means for protecting privacy and other rights, and beneficial uses of covered data by covered entities.

(f) LARGE DATA HOLDER METRICS REPORTING.—A large data holder that is a covered entity shall, for each calendar year in which it was a large data holder, do the following:

(1) 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 204(b).

(D) The number of requests to opt-out of targeted advertising under section 204(c).

(E) The number of requests in each of subparagraphs (A) through (D) that such large data holder (i) complied with in whole or in part and (ii) denied.

(F) The median or mean number of days within which such large data holder substantively responded to the requests in each of subparagraphs (A) through (D).

(2) Disclose by July 1 of each applicable calendar year the information compiled in paragraph (1) within such large data holder's privacy policy required under section 202 or on the publicly accessible website of such large data holder that is accessible from a hyperlink included in the privacy policy.

(g) REGULATIONS.—Not later than 2 years after the date of enactment of this Act, the Commission shall promulgate regulations, pursuant to section 553 of title 5, United States Code, as necessary to establish processes by which covered entities are to comply with the provisions of this section. Such regulations shall take into consideration—

(1) the size of, and the nature, scope, and complexity of the activities engaged in by the covered entity, including whether the covered entity is a large data holder, nonprofit organization, covered entity meeting the requirements of section 209, third party, or third-party collecting entity;

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

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

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

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

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

SEC. 204. RIGHT TO CONSENT AND OBJECT.

(a) WITHDRAWAL OF CONSENT.—A covered entity shall provide an individual with a clear and conspicuous, easy-to-execute means to withdraw any affirmative express consent previously provided by the individual that is as easy to execute by a reasonable individual as the means to provide consent, with respect to the processing or transfer of the covered data of the individual.

(b) RIGHT TO OPT OUT OF COVERED DATA TRANSFERS.—

(1) IN GENERAL.—A covered entity—

(A) may not transfer or direct the transfer of the covered data of an individual to a third party if the individual objects to the transfer; and

(B) shall allow an individual to object to such a transfer through an opt-out mechanism, as described in section 210.

(2) EXCEPTION.—Except as provided in section 206(b)(3)(C), a covered entity need not allow an individual to opt out of the collection, processing, or transfer of covered data made pursuant to the exceptions in paragraphs (1) through (15) of section 101(b).

(c) RIGHT TO OPT OUT OF TARGETED ADVERTISING.—

(1) A covered entity or service provider that directly delivers a targeted advertisement shall—

(A) prior to engaging in targeted advertising to an individual or device and at all times thereafter, provide such individual with a clear and conspicuous means to opt out of targeted advertising;

(B) abide by any opt-out designation by an individual with respect to targeted advertising and notify the covered entity that directed the service provider to deliver the targeted advertisement of the opt-out decision; and

(C) allow an individual to make an opt-out designation with respect to targeted advertising through an opt-out mechanism, as described in section 210.

(2) A covered entity or service provider that receives an opt-out notification pursuant to paragraph (1)(B) or this paragraph shall abide by such opt-out designations by an individual and notify any other person that directed the covered entity or service provider to serve, deliver, or otherwise handle the advertisement of the opt-out decision.

(d) INDIVIDUAL AUTONOMY.—A covered entity may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of any individual right under this section through—

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

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

SEC. 205. DATA PROTECTIONS FOR CHILDREN AND MINORS.

(a) PROHIBITION ON TARGETED ADVERTISING TO CHILDREN AND MINORS.—A covered entity may not engage in targeted advertising to any individual if the covered entity has knowledge that the individual is a covered minor.

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

(1) IN GENERAL.—A covered entity may not transfer or direct the transfer of the covered data of a covered minor to a third party if the covered entity—

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

(B) has not obtained affirmative express consent from the covered minor or the covered minor's parent or guardian.

(2) EXCEPTION.—A covered entity or service provider may collect, process, or transfer covered data of an individual the covered entity or service provider knows is under the age of 18 solely in order to submit information relating to child victimization to law enforcement or to the nonprofit, national resource center and clearinghouse congressionally designated to provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children issues.

(c) YOUTH PRIVACY AND MARKETING DIVISION.—

(1) ESTABLISHMENT.—There is established within the Commission in the privacy bureau established in this Act, a division to be known as the "Youth Privacy and Marketing Division" (in this section referred to as the "Division").

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

(3) DUTIES.—The Division shall be responsible for assisting the Commission in addressing, as it relates to this Act—

(A) the privacy of children and minors; and

(B) marketing directed at children and minors.

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

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

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

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

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

(d) REPORT BY THE INSPECTOR GENERAL.—

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

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

(i) operating fairly and effectively; and

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

(B) any proposal or recommendation for policy changes that would improve the effectiveness of the safe harbor provisions.

(2) PUBLICATION.—Not later than 10 days after the date on which a report is submitted under paragraph (1), the Commission shall publish the report on the website of the Commission.

SEC. 206. THIRD-PARTY COLLECTING ENTITIES.

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

(1) notifies individuals that the entity is a third-party collecting entity using specific language that the Commission shall develop through rulemaking under section 553 of title 5, United States Code;

(2) includes a link to the website established under subsection (b)(3); and

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

(b) THIRD-PARTY COLLECTING ENTITY REGISTRATION.—

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

(2) REGISTRATION REQUIREMENTS.—In registering with the Commission as required under paragraph (1), a third-party collecting entity 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 third-party collecting entity.

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

(iii) The contact information of the third-party collecting entity, including a contact person, a telephone number, an 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 provided under this subsection.

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

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

(B) For each registered third-party collecting entity, the information provided under paragraph (2)(B).

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

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

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

(ii) Each third-party collecting entity that receives such a request from an individual shall delete all the covered data of the individual not later than 30 days after the request is received by the third-party collecting entity.

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

(c) PENALTIES.—

(1) IN GENERAL.—A third-party collecting entity that fails to register or provide the notice as required under this section shall be liable for—

(A) a civil penalty of $100 for each day the third-party collecting entity fails to register or provide notice as required under this section, not to exceed a total of $10,000 for any year; and

(B) an amount equal to the registration fees due under paragraph (2)(A) of subsection (b) for each year that the third-party collecting entity failed to register as required under paragraph (1) of such subsection.

(2) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed as altering, limiting, or affecting any enforcement authorities or remedies under this Act.

SEC. 207. CIVIL RIGHTS AND ALGORITHMS.

(a) CIVIL RIGHTS PROTECTIONS.—

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

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

(A) the collection, processing, 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; or

(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)).

(b) FTC ENFORCEMENT ASSISTANCE.—

(1) IN GENERAL.—Whenever the Commission obtains information that a covered entity or service provider may have collected, processed, or transferred covered data in violation of subsection (a), the Commission shall transmit such in-

formation 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 harm to an individual or group of individuals, and uses such covered algorithm solely or in part, to collect, process, or transfer covered data shall conduct an impact assessment of such algorithm in accordance with 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 that is designed to, solely or in part, to collect, process, or transfer covered data in furtherance of a consequential decision shall prior to deploying the covered algorithm in interstate commerce evaluate the design, structure, and inputs of the covered algorithm, including any training data used to develop the covered algorithm, to reduce the risk of the potential harms identified under paragraph (1)(B).

(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).

(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, submit the impact assessment or evaluation conducted under paragraph (1) or (2) 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.—Covered entities and service providers may redact and segregate any trade secret (as defined in section 1839 of title 18, United States Code) or other confidential or proprietary information from public disclosure under this 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)) in regard to such information.

(C) ENFORCEMENT.—The Commission may not use any information obtained solely and exclusively through a covered entity or a service provider's disclosure of information to the Commission in compliance with this section for any purpose other than enforcing this Act with the exception of enforcing consent orders, including the study and report provisions in paragraph (6). This subparagraph does not preclude the Commission from providing this information to Congress in response to a subpoena.

(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, or their respective designees, publish guidance regarding compliance with this section.

(5) RULEMAKING AND EXEMPTION.—The Commission shall have authority under section 553 of title 5, United States Code, to promulgate regulations as necessary to establish processes by which a large data holder—

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

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

(6) STUDY AND REPORT.—

(A) STUDY.—The Commission, in consultation with the Secretary of Commerce or the Secretary's designee, shall conduct a study, to review any impact assessment or evaluation submitted under this 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 or the Secretary's designee, 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. 208. DATA SECURITY AND PROTECTION OF COVERED DATA.

(a) ESTABLISHMENT OF DATA SECURITY PRACTICES.—

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

(2) CONSIDERATIONS.—The reasonable administrative, technical, and physical 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 or the service provider's collecting, processing, or transferring of covered data;

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

(D) the sensitivity of the covered data collected, processed, or transferred;

(E) the current state of the art (and limitations thereof) in administrative, technical, and physical safeguards for protecting such covered data; and

(F) the cost of available tools to improve security and reduce vulnerabilities to unauthorized access and acquisition of such covered data in relation to the risks and nature of the covered data.

(b) SPECIFIC REQUIREMENTS.—The data security practices of the covered entity and of the service provider required under subsection (a) shall include, for each respective entity's own system or systems, at a minimum, the following practices:

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

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

(3) EVALUATION OF PREVENTIVE AND CORRECTIVE ACTION.—Evaluating and making reasonable adjustments to the action described in paragraph (2) in light of any material changes in technology, internal or external threats to covered data, and the covered entity or service provider's own changing business arrangements or operations.

(4) INFORMATION RETENTION AND DISPOSAL.—Disposing of covered data in accordance with a retention schedule that shall require the deletion of covered data when such data is required to be deleted by law or is no longer necessary for the purpose for which the data was collected, processed, or transferred, unless an individual has provided affirmative express consent to such retention. Such disposal shall include destroying, permanently erasing, or otherwise modifying the covered data to make such data permanently unreadable or indecipherable and unrecoverable to ensure ongoing compliance with this section. Service providers shall establish practices to delete or return covered data to a covered entity as requested at the end of the provision of services unless retention of the covered data is required by law, consistent with section 302(a)(6).

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

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

(7) INCIDENT RESPONSE.—Implementing procedures to detect, respond to, or recover from security incidents, including breaches.

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

SEC. 209. SMALL BUSINESS PROTECTIONS.

(a) ESTABLISHMENT OF EXEMPTION.—Any covered entity or service provider that can establish that it met the requirements described in subsection (b) for the period of the 3 preceding calendar years (or for the period during which the covered entity or service provider has been in existence if such period is less than 3 years) shall—

(1) be exempt from compliance with section 203(a)(4), paragraphs (1) through (3) and (5) through (7) of section 208(b), and section 301(c); and

(2) at the covered entity's sole discretion, have the option of complying with section 203(a)(2) by, after receiving a verified request from an individual to correct covered data of the individual under such section, deleting such covered data in its entirety instead of making the requested correction.

(b) EXEMPTION REQUIREMENTS.—The requirements of this subsection are, with respect to a covered entity or a service provider, the following:

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

(2) The covered entity or service provider, on average, did not annually collect or process the covered data of more than 200,000 individuals during the period beyond the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product, so long as all covered data for such purpose was deleted or de-identified within 90 days, except when necessary to investigate fraud or as consistent with a covered entity's return policy.

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

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

SEC. 210. UNIFIED OPT-OUT MECHANISMS.

(a) IN GENERAL.—For the rights established under subsection (b) of section 204, subsection (c) of section 204 (except as provided for under section 101(b)(16)), and section 206(b)(3)(C), following public notice and opportunity to comment and not later than 18 months after the date of enactment of this Act, the Commission shall establish or recognize one or more acceptable privacy protective, centralized mechanisms, including global privacy signals such as browser or device privacy settings, other tools offered by covered entities or service providers, and registries of identifiers, for individuals to exercise all such rights through a single interface for a covered entity or service provider to utilize to allow an individual to make such opt out designations with respect to covered data related to such individual.

(b) REQUIREMENTS.—Any such centralized opt-out mechanism shall—

(1) require covered entities or service providers acting on behalf of covered entities to inform individuals about the centralized opt-out choice;

(2) not be required to be the default setting, but may be the default setting provided that in all cases the mechanism clearly represents the individual's affirmative, freely given, and unambiguous choice to opt out;

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

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

(5) be provided in any covered language in which the covered entity provides products or services subject to the opt-out; and

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

TITLE III—CORPORATE ACCOUNTABILITY

SEC. 301. EXECUTIVE RESPONSIBILITY.

(a) IN GENERAL.—Beginning 1 year after the date of enactment of this Act, an executive officer of a large data holder shall annually certify, in good faith, to the Commission, in a manner specified by the Commission by regulation under section 553 of title 5, United States Code, that the entity maintains—

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

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

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

(c) DESIGNATION OF PRIVACY AND DATA SECURITY OFFICER.—

(1) IN GENERAL.—A covered entity or service provider that have more than 15 employees, shall designate—

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

(B) 1 or more qualified employees (in addition to any employee designated under subparagraph (A)) as data security officers.

(2) REQUIREMENTS FOR OFFICERS.—An employee who is designated by a covered entity or a service provider as a privacy officer or a data security officer pursuant to paragraph (1) shall, at a minimum—

(A) 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

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

(3) ADDITIONAL REQUIREMENTS FOR LARGE DATA HOLDERS.—A large data holder shall designate at least 1 of the officers described in paragraph (1) to report directly to the highest official at the large data holder as a privacy protection officer who shall, in addition to the requirements in paragraph (2), either directly or through a supervised designee or designees—

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

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

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

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

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

(d) LARGE DATA HOLDER PRIVACY IMPACT ASSESSMENTS.—

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

(2) ASSESSMENT REQUIREMENTS.—A privacy impact assessment required under paragraph (1) shall be—

(A) reasonable and appropriate in scope given—

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

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

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

(B) documented in written form and maintained by the large data holder unless rendered out of date by a subsequent assessment conducted under paragraph (1); and

(C) approved by the privacy protection officer designated in subsection (c)(3) of the large data holder, as applicable.

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

(e) OTHER PRIVACY IMPACT ASSESSMENTS.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act and biennially thereafter, each covered entity that is not large data holder and does not meet the requirements for covered entities under section 209 shall conduct a privacy impact assessment. Such assessment shall weigh the benefits of the covered entity's covered data collecting, processing, and transfer practices that may cause a substantial privacy risk against the potential material adverse consequences of such practices to individual privacy.

(2) ASSESSMENT REQUIREMENTS.—A privacy impact assessment required under paragraph (1) shall be—

(A) reasonable and appropriate in scope given—

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

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

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

(B) documented in written form and maintained by the covered entity unless rendered out of date by a subsequent assessment conducted under paragraph (1).

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

SEC. 302. SERVICE PROVIDERS AND THIRD PARTIES.

(a) SERVICE PROVIDERS.—A service provider—

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

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

(3) shall assist a covered entity in responding to a request made by an individual under section 203 or 204, by either—

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

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

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

(ii) providing written verification to the covered entity that it does not hold covered data related to the request, that complying with the request would be inconsistent with its legal obligations, or that the request falls within an exception to section 203 or 204;

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

(5) shall, upon the reasonable request of the covered entity, make available to the covered entity information necessary to demonstrate the compliance of the service provider with the requirements of this Act, which may include making available a report of an independent assessment arranged by the service provider on terms agreed to by the service provider and the covered entity, providing information necessary to enable the covered entity to conduct and document a privacy impact assessment required by subsection (d) or (e) of section 301, and making available the report required under section 207(c)(2);

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

(7) 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 208; and

(8) shall allow and cooperate with, reasonable assessments by the covered entity or the covered entity's designated assessor; alternatively, the service provider may arrange for a qualified and independent assessor to conduct an as-

sessment 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. The service provider shall provide a report of such assessment to the covered entity upon request.

(b) CONTRACTS BETWEEN COVERED ENTITIES AND SERVICE PROVIDERS.—

(1) REQUIREMENTS.—A person or entity may only act as a service provider pursuant to a written contract between the covered entity and the service provider, or a written contract between one service provider and a second service provider as described under subsection (a)(4), if the contract—

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

(B) clearly sets forth—

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

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

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

(iv) the duration of processing; and

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

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

(D) prohibits—

(i) collecting, processing, or transferring covered data in contravention to subsection (a); and

(ii) combining service provider data with covered data which the service provider receives from or on behalf of another person or persons or collects from the interaction of the service provider with an individual, provided that such combining is not necessary to effectuate a purpose described in paragraphs (1) through (15) of section 101(b) and is otherwise permitted under the contract required by this subsection.

(2) CONTRACT TERMS.—Each service provider shall retain copies of previous contracts entered into in compliance with this subsection with each covered entity to which it provides requested products or services.

(c) RELATIONSHIP BETWEEN COVERED ENTITIES AND SERVICE PROVIDERS.—

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

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

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

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

(d) THIRD PARTIES.—A third party—

(1) shall not process third party data for a processing purpose other than, in the case of sensitive covered data, the processing purpose for which the individual gave affirmative express consent or to effect a purpose enumerated in paragraph (1), (3), or (5) of section 101(b) and, in the case of non-sensitive data, the processing purpose for which the covered entity made a disclosure pursuant to section 202(b)(4); and

(2) for purposes of paragraph (1), may reasonably rely on representations made by the covered entity that transferred the third party data if the third

party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible.

(e) ADDITIONAL OBLIGATIONS ON COVERED ENTITIES.—

(1) IN GENERAL.—A covered entity or service provider shall exercise reasonable due diligence in—

(A) selecting a service provider; and

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

(2) GUIDANCE.—Not later than 2 years after the date of enactment of this Act, the Commission shall publish guidance regarding compliance with this subsection, taking into consideration the burdens on large data holders, covered entities who are not large data holders, and covered entities meeting the requirements of section 209.

(f) RULE OF CONSTRUCTION.—Solely for the purposes of this section, the requirements for service providers to contract with, assist, and follow the instructions of covered entities shall be read to include requirements to contract with, assist, and follow the instructions of a government entity if the service provider is providing a service to a government entity.

SEC. 303. TECHNICAL COMPLIANCE PROGRAMS.

(a) IN GENERAL.—Not later than 3 years after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to establish a process for the proposal and approval of technical compliance programs under this section used by a covered entity to collect, process, or transfer covered data.

(b) SCOPE OF PROGRAMS.—The technical compliance programs established under this section shall, with respect to a technology, product, service, or method used by a covered entity to collect, process, or transfer covered data—

(1) establish publicly available guidelines for compliance with this Act; and

(2) meet or exceed the requirements of this Act.

(c) APPROVAL PROCESS.—

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

(2) EXPEDITED RESPONSE TO REQUESTS.—Beginning 1 year after the date of enactment of this Act, the Commission shall act upon a request for the proposal and approval of a technical compliance program not later than 1 year after the filing of the request, and shall set forth publicly in writing the conclusions of the Commission with regard to such request.

(d) RIGHT TO APPEAL.—Final action by the Commission on a request for approval, amendment, or repeal of a technical compliance program, or the failure to act within the 1-year period after a request for approval, amendment, or repeal of a technical compliance program is made under subsection (c), may be appealed to a Federal district court of the United States of appropriate jurisdiction as provided for in section 702 of title 5, United States Code.

(e) EFFECT ON ENFORCEMENT.—

(1) IN GENERAL.—Prior to commencing an investigation or enforcement action against any covered entity under this Act, the Commission and State attorney general shall consider the covered entity's history of compliance with any technical compliance program approved under this section and any action taken by the covered entity to remedy noncompliance with such program. If such enforcement action described in section 403 is brought, the covered entity's history of compliance with any technical compliance program approved under this section and any action taken by the covered entity to remedy noncompliance with such program shall be taken into consideration when determining liability or a penalty. The covered entity's history of compliance with any technical compliance program shall not affect any burden of proof or the weight given to evidence in an enforcement or judicial proceeding.

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

(3) RULE OF CONSTRUCTION.—Nothing in this subsection shall provide any individual, class of individuals, or person with any right to seek discovery of any non-public Commission deliberation or activity or impose any pleading requirement on the Commission if the Commission brings an enforcement action of any kind.

SEC. 304. COMMISSION APPROVED COMPLIANCE GUIDELINES.

(a) APPLICATION FOR COMPLIANCE GUIDELINE APPROVAL.—

(1) IN GENERAL.—A covered entity that is not a third-party collecting entity and meets the requirements of section 209, or a group of such covered entities, may apply to the Commission for approval of 1 or more sets of compliance guidelines governing the collection, processing, and transfer of covered data by the covered entity or group of covered entities.

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

(A) a description of how the proposed 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 that meet the requirements of section 209 and are not third-party collecting entities, if any are known at the time of application, that intend to adhere to the compliance guidelines; and

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

(3) COMMISSION REVIEW.—

(A) INITIAL APPROVAL.—

(i) PUBLIC COMMENT PERIOD.—Within 90 days after the receipt of proposed guidelines submitted pursuant to paragraph (2), the Commission shall publish the application and provide an opportunity for public comment on such compliance guidelines.

(ii) APPROVAL.—The Commission shall approve an application regarding proposed guidelines under paragraph (2) if the applicant demonstrates that the compliance guidelines—

(I) meet or exceed requirements of this Act;

(II) provide for the regular review and validation by an independent organization not associated with any of the covered entities that may participate in the guidelines and that is approved by the Commission to conduct such reviews of the compliance guidelines of the covered entity or entities to ensure that the covered entity or entities continue to meet or exceed the requirements of this 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 401 or referral to the appropriate State attorney general for enforcement consistent with section 402.

(iii) TIMELINE.—Within 1 year after receiving an application regarding proposed guidelines under paragraph (2), the Commission shall issue a determination approving or denying the application and providing its reasons for approving or denying such application.

(B) APPROVAL OF MODIFICATIONS.—

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

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

(b) WITHDRAWAL OF APPROVAL.—If at any time the Commission determines that the guidelines previously approved no longer meet the requirements of this Act or a regulation promulgated under this Act or that compliance with the approved guidelines is insufficiently enforced by the independent organization administering the guidelines, the Commission shall notify the covered entities or group of such entities and the independent organization of the determination of the Commission to withdraw approval of such guidelines and the basis for doing so. Within180 days after receipt of such notice, the covered entity or group of such entities and the independent organization may cure any alleged deficiency with the guidelines or the enforcement of such guidelines and submit each proposed cure to the Commission. If the Commission determines that such cures eliminate the alleged deficiency in the guidelines, then the Commission may not withdraw approval of such guidelines on the basis of such determination.

(c) DEEMED COMPLIANCE.—A covered entity that is eligible to participate under subsection (a)(1) and participates in guidelines approved under this section shall be deemed in compliance with the relevant provisions of this Act if such covered entity is in compliance with such guidelines.

SEC. 305. DIGITAL CONTENT FORGERIES.

(a) REPORTS.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Secretary of Commerce or the Secretary's designee shall publish a report regarding digital content forgeries.

(b) REQUIREMENTS.—Each report under subsection (a) shall include the following:

(1) A definition of digital content forgeries along with accompanying explanatory materials.

(2) A description of the common sources of digital content forgeries in the United States and commercial sources of digital content forgery technologies.

(3) An assessment of the uses, applications, and harms of digital content forgeries.

(4) An analysis of the methods and standards available to identify digital content forgeries as well as a description of the commercial technological countermeasures that are, or could be, used to address concerns with digital content forgeries, which may include the provision of warnings to viewers of suspect content.

(5) A description of the types of digital content forgeries, including those used to commit fraud, cause harm, or violate any provision of law.

(6) Any other information determined appropriate by the Secretary of Commerce or the Secretary's designee.

TITLE IV—ENFORCEMENT, APPLICABILITY, AND MISCELLANEOUS

SEC. 401. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) BUREAU OF PRIVACY.—

(1) IN GENERAL.—The Commission shall establish within the Commission a new bureau to be known as the "Bureau of Privacy", which shall be of similar structure, size, organization, and authority as the existing bureaus within the Commission related to consumer protection and competition.

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

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

(b) OFFICE OF BUSINESS MENTORSHIP.—The Director of the Bureau established under subsection (a)(1) shall establish within the Bureau an office to be known as the "Office of Business Mentorship" to provide guidance and education to covered entities and service providers regarding compliance with this Act. Covered entities or service providers may request advice from the Commission or the Office with respect to a course of action that the covered entity or service provider proposes to pursue and that may relate to the requirements of this Act.

(c) 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), (4), and (5), 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 person who 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) LIMITING CERTAIN ACTIONS UNRELATED TO THIS ACT.—If the Commission brings a civil action alleging that an act or practice violates this Act or a regulation promulgated under this Act, the Commission may not seek a cease and de-

sist order against the same defendant under section 5(b) of the Federal Trade Commission Act (15 U.S.C. 45(b)) to stop that same act or practice on the grounds that such act or practice constitutes an unfair or deceptive act or practice.

(4) COMMON CARRIERS AND NONPROFIT ORGANIZATIONS.—Notwithstanding any jurisdictional limitation of the Commission with respect to consumer protection or privacy, the Commission shall enforce this Act and the regulations promulgated under this Act, in the same manner provided in paragraphs (1), (2), (3), and (5), with respect to common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof and supplementary thereto and organizations not organized to carry on business for their own profit or that of their members.

(5) 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" in this paragraph referred to as the "Victims Relief Fund".

(B) DEPOSITS.—Notwithstanding section 3302 of title 31, United States Code, in any judicial or administrative action to enforce this Act or a regulation promulgated under this Act, the amount of any civil penalty obtained against a covered entity or service provider, or any other monetary relief ordered to be paid by a covered entity or service provider to provide redress, payment, compensation, or other relief to individuals that cannot be located or the payment of which would otherwise not be practicable, shall be deposited into the Victims Relief Fund.

(C) USE OF FUNDS.—

(i) USE BY COMMISSION.—Amounts in the Victims Relief Fund shall be available to the Commission, without fiscal year limitation, to provide redress, payment, compensation, or other monetary relief to individuals affected by an act or practice for which relief has been obtained under this Act.

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

(I) funding the activities of the Office of Business Mentorship established under subsection (b); or

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

SEC. 402. ENFORCEMENT BY STATES.

(a) CIVIL ACTION.—In any case in which the attorney general or State Privacy Authority of a State has reason to believe that an interest of the residents of that State has been, may be, or is adversely affected by a violation of this Act or a regulation promulgated under this Act by a covered entity or service provider, the attorney general or State Privacy Authority may bring a civil action in the name of the State, or as parens patriae on behalf of the residents of the State. Any such action shall be brought exclusively in an appropriate Federal district court of the United States to—

(1) enjoin such act or practice;

(2) enforce compliance with this Act or such regulation;

(3) obtain damages, civil penalties, restitution, or other compensation on behalf of the residents of such State; or

(4) obtain reasonable attorneys' fees and other litigation costs reasonably incurred.

(b) RIGHTS OF THE COMMISSION.—

(1) IN GENERAL.—Except as provided in paragraph (2), the attorney general or State Privacy Authority of a State shall notify the Commission in writing prior to initiating a civil action under subsection (a). Such notification shall include a copy of the complaint to be filed to initiate such action. Upon receiving such notification, the Commission may intervene in such action as a matter of right pursuant to the Federal Rules of Civil Procedure.

(2) FEASIBILITY.—If the notification required by paragraph (1) is not feasible, the attorney general or State Privacy Authority 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 violation of this Act or a regulation promulgated under this Act, no attorney general or State Privacy Authority of a State 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, if such complaint alleges such violation affected the residents of such State or individuals nationwide. If the Commission brings a civil action against a covered entity or service provider for a violation of this Act or a regulation promulgated under this Act that affects the interests of the residents of a State, the attorney general or State Privacy Authority of such State may intervene in such action as a matter of right pursuant to the Federal Rules of Civil Procedure.

(d) RULE OF CONSTRUCTION.—Nothing in this section may be construed to prevent the attorney general or State Privacy Authority of a State from exercising the powers conferred on the attorney general or State Privacy Authority to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

(e) PRESERVATION OF STATE POWERS.—Except as provided in subsection (c), nothing in this section may be construed as altering, limiting, or affecting the authority of the attorney general or State Privacy Authority of a State to—

(1) bring an action or other regulatory proceeding arising solely under the law in effect in the State that is preempted by this Act or under another applicable Federal law; or

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

SEC. 403. ENFORCEMENT BY PERSONS.

(a) ENFORCEMENT BY PERSONS.—

(1) IN GENERAL.—Beginning on the date that is 2 years after the date on which this Act takes effect, any person or class of persons for a violation of this Act or a regulation promulgated under this Act by a covered entity or service provider may bring a civil action against such entity in any Federal court of competent jurisdiction.

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

(A) an amount equal to the sum of any compensatory damages;

(B) injunctive relief;

(C) declaratory relief; and

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

(3) RIGHTS OF THE COMMISSION AND STATE ATTORNEYS GENERAL.—

(A) IN GENERAL.—Prior to a person bringing a civil action under paragraph (1), such person shall notify the Commission and the attorney general of the State where such person resides in writing that such person intends to bring a civil action under such paragraph. Upon receiving such notice, the Commission and State attorney general shall each or jointly make a determination and respond to such person not later than 60 days after receiving such notice, as to whether they will intervene in such action pursuant to the Federal Rules of Civil Procedure. If a state attorney general does intervene, they shall only be heard with respect to the interests of the residents of their State

(B) RETAINED AUTHORITY.—Subparagraph (A) may not be construed to limit the authority of the Commission or any applicable State attorney general or State Privacy Authority to later commence a proceeding or civil action or intervene by motion if the Commission or State attorney general or State Privacy Authority does not commence a proceeding or civil action within the 60-day period.

(C) BAD FAITH.—Any written communication from counsel for an aggrieved party to a covered entity or service provider requesting a monetary payment from that covered entity or service provider regarding a specific claim described in a letter sent pursuant to subsection (d), not including filings in court proceedings, arbitrations, mediations, judgment collection processes, or other communications related to previously initiated litigation or arbitrations, shall be considered to have been sent in bad faith and shall be unlawful as defined in this Act, if the written communication was sent prior to the date that is 60 days after either a State attorney general or the Commission has received the notice required under subparagraph (A).

(4) FTC STUDY.—Beginning on the date that is 5 years after the date of enactment of this Act and every 5 years thereafter, the Commission's Bureau of Economics and Bureau of Privacy shall assist the Commission in conducting a study to determine the economic impacts in the United States of demand letters sent pursuant to this section and the scope of the rights of a person under this

section to bring forth civil actions against covered entities and service providers. Such study shall include the following:

(A) The impact on insurance rates in the United States.

(B) The impact on the ability of covered entities to offer new products or services.

(C) The impact on the creation and growth of new startup companies, including new technology companies.

(D) Any emerging risks, benefits, and long-term trends in relevant marketplaces, supply chains, and labor availability.

(E) The impact on reducing, preventing, or remediating harms to individuals, including from fraud, identity theft, spam, discrimination, defective products, and violations of rights.

(F) The impact on the volume and severity of data security incidents, and the ability to respond to data security incidents.

(G) Other intangible direct and indirect costs and benefits to individuals.

(5) REPORT TO CONGRESS.—Not later than 5 years after the first day on which persons and classes of persons are able to bring civil actions under this subsection, and annually thereafter, the Commission shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report that contains the results of the study conducted under paragraph (4).

(b) ARBITRATION AGREEMENTS AND PRE-DISPUTE JOINT ACTION WAIVERS.—

(1) PRE-DISPUTE ARBITRATION AGREEMENTS.—

(A) Notwithstanding any other provision of law, no pre-dispute arbitration agreement with respect to an individual under the age of 18 is enforceable with regard to a dispute arising under this Act.

(B) Notwithstanding any other provision of law, no pre-dispute arbitration agreement is enforceable with regard to a dispute arising under this Act concerning a claim related to gender or partner-based violence or physical harm.

(2) PRE-DISPUTE JOINT-ACTION WAIVERS.—Notwithstanding any other provision of law, no pre-dispute joint-action waiver with respect to an individual under the age of 18 is enforceable with regard to a dispute arising under this Act.

(3) DEFINITIONS.—For purposes of this subsection:

(A) PRE-DISPUTE ARBITRATION AGREEMENT.—The term "pre-dispute arbitration agreement" means any agreement to arbitrate a dispute that has not arisen at the time of the making of the agreement.

(B) PRE-DISPUTE JOINT-ACTION WAIVER.—The term "pre-dispute joint-action waiver" means an agreement, whether or not part of a pre-dispute arbitration agreement, that would prohibit or waive the right of 1 of the parties to the agreement to participate in a joint, class, or collective action in a judicial, arbitral, administrative, or other related forum, concerning a dispute that has not yet arisen at the time of the making of the agreement.

(c) RIGHT TO CURE.—

(1) NOTICE.—Subject to paragraph (3), with respect to a claim under this section for—

(A) injunctive relief; or

(B) an action against a covered entity or service provider that meets the requirements of section 209 of this Act, such claim may be brought by a person or class of persons if—prior to asserting such claim—the person or class or persons provides to the covered entity or service provider 45 days' written notice identifying the specific provisions of this Act the person or class of persons alleges have been or are being violated.

(2) EFFECT OF CURE.—Subject to paragraph (3), in the event a cure is possible, if within the 45 days the covered entity or service provider demonstrates to the court that it has cured the noticed violation or violations and provides the person or class of persons an express written statement that the violation or violations has been cured and that no further violations shall occur, a claim for injunctive relief shall not be permitted and may be reasonably dismissed.

(3) RULE OF CONSTRUCTION.—The notice described in paragraph (1) and the reasonable dismissal in paragraph (2) shall not apply more than once to any alleged underlying violation by the same covered entity.

(d) DEMAND LETTER.—If a person or a identified members of a class of persons represented by counsel in regard to an alleged violation or violations of the Act and has correspondence sent to a covered entity or service provider by counsel alleging a violation or violations of the provisions of this Act and requests a monetary payment, such correspondence shall include the following language: "Please visit the website of the Federal Trade Commission for a general description of your rights

under the American Data Privacy and Protection Act" followed by a hyperlink to the webpage of the Commission required under section 201. If such correspondence does not include such language and hyperlink, a civil action brought under this section by such person or identified members of the class of persons represented by counsel may be dismissed without prejudice and shall not be reinstated until such person or persons has complied with this subsection.

(e) APPLICABILITY.—

(1) IN GENERAL.—This section shall only apply to a claim alleging a violation of section 102, 104, 202, 203, 204, 205(a), 205(b), 206(b)(3)(C), 207(a), 208(a), or 302, or a regulation promulgated under any such section.

(2) EXCEPTION.—This section shall not apply to any claim against a covered entity that has less than $25,000,000 per year in revenue, collects, processes, or transfers the covered data of fewer than 50,000 individuals, and derives less than 50 percent of its revenue from transferring covered data.

SEC. 404. RELATIONSHIP TO FEDERAL AND STATE LAWS.

(a) 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) FULL APPLICATION OF THE ANTITRUST LAW.—Nothing in this Act may be construed to modify, impair or supersede the operation of the antitrust law or any other provision of law.

(B) NO IMMUNITY FROM THE ANTITRUST LAW.—Nothing in the regulatory regime adopted by this Act shall be construed as operating to limit any law deterring anticompetitive conduct or diminishing the need for full application of the antitrust law. Nothing in this Act explicitly or implicitly precludes the application of the antitrust law.

(C) DEFINITION OF ANTITRUST LAW.—For purposes of this section, the term antitrust law has the same meaning as in subsection (a) of the first section of the Clayton Act (15 U.S.C. 12), except that such term includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that such section 5 applies to unfair methods of competition.

(3) APPLICABILITY OF OTHER PRIVACY REQUIREMENTS.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.), the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), the Family Educational Rights and Privacy Act (20 U.S.C. 1232g; part 99 of title 34, Code of Federal Regulations) to the extent such covered entity is a school as defined in 20 U.S.C. 1232g(a)(3) or 34 C.F.R. 99.1(a), section 444 of the General Education Provisions Act (commonly known as the "Family Educational Rights and Privacy Act of 1974") (20 U.S.C. 1232g) and part 99 of title 34, Code of Federal Regulations (or any successor regulation), the Confidentiality of Alcohol and Drug Abuse Patient Records at 42 U.S.C. 290dd-2 and its implementing regulations at 42 CFR part 2, the Genetic Information Non-discrimination Act (GINA), or 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), and is in compliance with the data privacy requirements of such regulations, part, title, or Act (as applicable), shall be deemed to be in compliance with the related requirements of this Act, except for section 208, solely and exclusively with respect to data subject to the requirements of such regulations, part, title, or Act. Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance describing the implementation of this paragraph.

(4) APPLICABILITY OF OTHER DATA SECURITY REQUIREMENTS.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.), or 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), and is in compliance with the information security

requirements of such regulations, part, title, or Act (as applicable), shall be deemed to be in compliance with the requirements of section 208, solely and exclusively with respect to data subject to the requirements of such regulations, part, title, or Act. Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance describing the implementation of this paragraph.

(b) PREEMPTION OF STATE LAWS.—

(1) IN GENERAL.—No State or political subdivision of a State may adopt, maintain, enforce, prescribe, or continue in effect any law, regulation, rule, standard, requirement, or other provision having the force and effect of law of any State, or political subdivision of a State, covered by the provisions of this Act, or a rule, regulation, or requirement promulgated under this Act.

(2) STATE LAW PRESERVATION.—Paragraph (1) may not be construed to preempt, displace, or supplant the following State laws, rules, regulations, or requirements:

(A) Consumer protection laws of general applicability, such as laws regulating deceptive, unfair, or unconscionable practices, except that the fact of a violation of this Act or a regulation promulgated under this Act may not be pleaded as an element of any violation of such a law.

(B) Civil rights laws.

(C) Provisions of laws, in so far as, that govern the privacy rights or other protections of employees, employee information, students, or student information.

(D) Laws that address notification requirements in the event of a data breach.

(E) Contract or tort law.

(F) Criminal laws.

(G) Civil laws governing fraud, theft (including identity theft), unauthorized access to information or electronic devices, unauthorized use of information, malicious behavior, or similar provisions of law.

(H) Civil laws regarding cyberstalking, cyberbullying, nonconsensual pornography, sexual harassment, child abuse material, child pornography, child abduction or attempted child abduction, coercion or enticement of a child for sexual activity, or child sex trafficking.

(I) Public safety or sector specific laws unrelated to privacy or security.

(J) Provisions of law, insofar as such provisions address public records, criminal justice information systems, arrest records, mug shots, conviction records, or non-conviction records.

(K) Provisions of law, insofar as such provisions address banking records, financial records, tax records, Social Security numbers, credit cards, consumer and credit reporting and investigations, credit repair, credit clinics, or check-cashing services.

(L) Provisions of law, insofar as such provisions address facial recognition or facial recognition technologies, electronic surveillance, wiretapping, or telephone monitoring.

(M) The Biometric Information Privacy Act (740 ICLS 14 et seq.) and the Genetic Information Privacy Act (410 ILCS 513 et seq.).

(N) Provisions of laws, in so far as, such provisions to address unsolicited email or text messages, telephone solicitation, or caller identification.

(O) Provisions of laws, in so far as, such provisions address health information, medical information, medical records, HIV status, or HIV testing.

(P) Provisions of laws, in so far as, such provisions pertain to public health activities, reporting, data, or services.

(Q) Provisions of law, insofar as such provisions address the confidentiality of library records.

(R) Section 1798.150 of the California Civil Code (as amended on November 3, 2020 by initiative Proposition 24, Section 16).

(S) Laws pertaining to the use of encryption as a means of providing data security.

(3) CPPA ENFORCEMENT.—Notwithstanding any other provisions of law, the California Privacy Protection Agency established under 1798.199.10(a) of the California Privacy Rights Act may enforce this Act, in the same manner, it would otherwise enforce the California Consumer Privacy Act, Section 1798.1050 et. seq.

(4) NONAPPLICATION OF FCC PRIVACY LAWS AND REGULATIONS TO CERTAIN COVERED ENTITIES.—Notwithstanding any other provision of law, sections 222, 338(i), and 631 of the Communications Act of 1934 (47 U.S.C. 222; 338(i); 551), and any regulations and orders promulgated by the Federal Communications Commission under any such section, do not apply to any covered entity with re-

spect to the collection, processing, transfer, or security of covered data or its equivalent, and the related privacy and data security activities of a covered entity that would otherwise be regulated under such sections shall be governed exclusively by the provisions of this Act, except for—

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

(B) subsections (b) and (g) of section 222 of the Communications Act of 1934 (47 U.S.C. 222); and

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

(c) PRESERVATION OF COMMON LAW OR STATUTORY CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this Act, nor any amendment, standard, rule, requirement, assessment, or regulation promulgated under this Act, may be construed to preempt, displace, or supplant any Federal or State common law rights or remedies, 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, 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.

SEC. 405. SEVERABILITY.

If any provision of this Act, or the application thereof to any person or circumstance, is held 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 by the invalidation.

SEC. 406. COPPA.

(a) IN GENERAL.—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.).

(b) UPDATED REGULATIONS.—Not later than 180 days after the date of enactment of this Act, the Commission shall amend its rules issued pursuant to the regulations promulgated by the Commission under the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.) to make reference to the additional requirements placed on covered entities under this Act, in addition to the requirements under the Children's Online Privacy Protection Act of 1998 that may already apply to certain covered entities.

SEC. 407. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Commission such sums as may be necessary to carry out this Act.

SEC. 408. EFFECTIVE DATE.

This Act shall take effect on the date that is 180 days after the date of enactment of this Act.

I. PURPOSE AND SUMMARY

H.R. 8152, the "American Data Privacy and Protection Act," establishes a preemptive national consumer privacy and data security framework built around limitations for collecting, processing, and transferring individuals' information, obligations for covered entities and service providers, and providing individuals with control with respect to their personal information. Certain covered data is considered sensitive and subject to additional restrictions and there are further protections for minors under 17 years old. Covered entities may not use covered data in any manner that discriminates or makes unavailable the equal enjoyment of goods or services on the basis of protected classes. Large businesses are subject to additional requirements while small and midsize businesses are exempted from certain provisions and eligible to participate in certain technical compliance programs. The Federal Trade Commission (FTC) is the primary federal regulator tasked with administration. H.R. 8152 provides for federal, state, and private enforcement.

II. BACKGROUND AND NEED FOR LEGISLATION

Advances in modern technologies have created unparalleled advances in consumer goods and services, and the level and detail of personal information entities now collect has followed suit. Accordingly, the lack of a national consumer privacy and data security standard is more pronounced in this increasingly digital world. One 2021 study showed that 70 percent of companies increased their collection of personal consumer data despite 86 percent of consumers citing data privacy as a growing concern.[1]

With the increase of data collection and skyrocketing value of personal information, many countries have passed comprehensive legislation to address privacy and data security. For instance, in 2016, the European Union adopted the General Data Protection Regulation (GDPR), in 2018, Brazil passed the General Data Protection Law, and in 2021, the People's Republic of China passed the Personal Information Protection Law. To date, over 100 countries have their own version of a comprehensive privacy and data security law, with many incorporating requirements from the GDPR in the absence of a U.S. law, such as Canada, the United Kingdom, and India. While other countries have led in national laws protecting personal information, the United States does not have a national consumer privacy and data security standard.

Instead, the United States generally relies on sector-specific privacy-related federal statutes that establish varying degrees of privacy and data security protections, impose different collection and use limitations on various entities, and provide consumers with varying degrees of individual rights.[2] These laws include: the Health Insurance Portability and Accountability Act, which protects information collected by a health care provider, health plan, health care clearinghouse, and the business associates of such entities;[3] the Family Educational Rights and Privacy Act, which regulates the collection of student data by public school officials and those they designate;[4] the Children's Online Privacy Protection Act of 1998 (COPPA), which covers data for children aged 12 and under with respect to online services directed to children;[5] the Genetic Information Nondiscrimination Act, which prohibits misuse of genetic data in employment or insurance decisions;[6] and the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act, which apply to financial institutions and credit reporting agencies.[7]

Many different types of data and entities are not covered by those or other sector-specific laws. To bridge those gaps, Congress must pass a national, comprehensive consumer privacy and data security law. To date, Americans have been forced to rely on the FTC's unfair or deceptive acts or practices authority under section 5 of the FTC Act.[8]

---

[1] KPMG, *Corporate Data Responsibility: Bridging the Consumer Trust Gap* (Aug. 2021) (https://advisory.kpmg.us/articles/2021/bridging-the-trust-chasm.html).
[2] Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries, Seattle* University Law Review (Apr. 9, 2019).
[3] Health Insurance Portability and Accountability Act, Pub. L. No. 104–191.
[4] 20 U.S.C. § 1232g.
[5] 15 U.S.C. § 6501, et seq.
[6] Genetic Information Nondiscrimination Act, Pub. L. No. 110–233.
[7] 15 U.S.C. §§ 6801–6809; 15 U.S.C. § 1681 et seq.
[8] 15 U.S.C. § 45.

The FTC authority is limited to cases in which: (i) the agency can prove substantial, unavoidable injury from conduct not outweighed by benefits to consumers or competition; or (ii) companies fail to live up to their own promises regarding data practices, regardless of whether such practices themselves are harmful.[9] There is no federal requirement for entities to make any such promises.[10]

The FTC is also limited in the relief it may obtain. The agency lacks first-offense civil penalty authority outside of very limited circumstances such as violations of regulations. The Supreme Court unanimously held in April 2021 that the FTC exceeded their authority and determined that the FTC may not obtain monetary relief for consumers who have been harmed solely by using the agency's authority under section 13(b) of the FTC Act.[11]

A growing number of states have tried to fill the federal consumer privacy and data security void by passing laws addressing consumer privacy and data security protections, including California, Virginia, Colorado, Utah, and Connecticut. These state laws materially vary in their scope, protections, obligations, and enforcement mechanisms.[12]

One consequence of the current state by state approach to comprehensively regulating consumer privacy and data security is that many entities do not have the resources or wherewithal to comply with numerous state laws that have conflicting requirements. One organization recently concluded that absent a national consumer privacy law, the growing patchwork of state consumer privacy laws may burden companies with multiple, duplicative compliance costs. This organization estimates that the out-of-state costs from every state passing a comprehensive consumer privacy law could exceed $1 trillion over ten years, with at least $200 billion hitting small businesses.[13]

The lack of a national consumer privacy framework also means that businesses may generally monitor themselves without regulatory oversight and collect, use, share, or sell data without meaningful limits on what is permitted. In many cases, this includes an individual's most sensitive personal information such as health information, precise geolocation history, and government-issued identifiers like social security numbers. Furthermore, once that data is in the hands of third parties it may be further sold, combined, and used, often without the individual's knowledge or consent.[14]

Additionally, the sectoral approach to regulating data privacy at the federal level does not provide national baseline anti-discrimination protections regarding the use of personal information. Although the Supreme Court has repeatedly affirmed that individuals are entitled to protection of their privacy regardless of changes in technology and that an individual's personal information may

---

[9] Federal Trade Commission, *FTC Report to Congress on Privacy and Security* (Sep. 13, 2021).
[10] *Id.*
[11] *AMG Capital Mgmt., LLC v. FTC*, 141 U.S. 1341 (2021).
[12] Mayer Brown, *Connecticut Passes Comprehensive Privacy Law: Comparing to Other States*, (www.mayerbrown.com/en/perspectives-events/publications/2022/05/connecticut-passes-comprehensive-privacy-law-comparing-to-other-state-privacy-laws) (May 11, 2022).
[13] Daniel Castro et al., *The Looming Cost of a Patchwork of State Privacy Laws,* Information Technology and Innovation Foundation (ITIF), (https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/) (Jan. 24, 2022).
[14] *The State of Consumer Data Privacy Laws in the US (and Why It Matters),* New York Times (Sept. 6, 2021).

not be used against them improperly, these concerns persist.[15] Federal law does not currently extend prohibitions to all instances of collecting, processing, or transferring covered data in any manner that discriminates in the provision of goods and services on the basis of protected classes in line with Supreme Court precedent.[16]

Online privacy harms are well-documented, including unwanted observation from excessive data collection and secondary use, discrimination, harms to children and teens from manipulation and targeting, thwarted consumer expectations, and more.[17] Americans are increasingly concerned by the tradeoff of providing their data in exchange for products and services, with 73 percent now saying this is an "unjustified use" of their information.[18]

As more data is collected on individuals by more products and services necessary for everyday life, Americans are subject to more risks from bad actors seeking to abuse lax privacy and data security regulation. As more data is collected by Big Tech on individuals by more products and services necessary for everyday life, Americans are subject to more risks. In the absence of federal consumer privacy and data security laws, that delineate best practices, Big Tech CEOs determine such practices on their own. This has created an environment where Big Tech also entices user's dependency on their platforms through products like password managers and de facto identities that follow users across the internet. As such products have become essential to an individual's ability to access their virtual lives, Big Tech's data collection and usage practices have positioned them to scrape and benefit from vast troves of personal information.[19]

The coronavirus disease of 2019 (COVID–19) pandemic exacerbated these concerns, particularly for children. During the pandemic, schools drastically increased the use of certain technologies as tools to aid learning while children attended school remotely, and one study found that 90 percent of these remote learning tools recommended by schools tracked students and sent their information to advertising companies.[20]

As children were unable to return to school, many took solace in social media platforms to interact with their classmates and friends. Platforms that collect more and more data in order to direct more content to increase children and teen's activity have created a toxic environment for them. This is particularly problematic for teen girls, who have been made especially vulnerable as social media platforms use engagement tools and algorithmically recommended content to emphasize body image, leading to decreased

---

[15] *See,* e.g., *Olmstead v. United States*, 277 U.S. 471 (1928) (Brandeis, J. dissenting); *Katz v. United States*, 389 U.S. 437 (1967); *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *NAACP v. Alabama,* 357 U.S. 449 (1958).

[16] *See,* e.g., *Shelley v. Kramer,* 334 U.S. 1 (1948); *Havens Realty Corp. v. Coleman*, 455 U.S. 363 (1982); *Pittsburgh Press Co. v. Pittsburgh Commission on Human Relations*, 413 U.S. 376 (1973); *Lawrence v. Texas*, 539 U.S. 558 (2003); *Bostock v. Clayton County,* 140 S. Ct. 1731 (2020).

[17] *6 Examples of Online Privacy Violation*, Cyber News (Apr. 15, 2020); Danielle Keats Citron & Daniel J. Solove, Privacy Harms, 102 Boston Univ. L. Rev. Online 793, 848 (2021)

[18] *Americans Widely Distrust Facebook, TikTok and Instagram with Their Data, Poll Finds*, Washington Post (Dec. 22, 2021).

[19] *The Security Risks of Logging in With Facebook*, Wired (Apr. 19, 2018).

[20] *Remote Learning Apps Shared Children's Data at a 'Dizzying Scale,'* Washington Post (May 24, 2022).

self-worth, higher rates of suicide, and other harmful mental health effects.[21]

Moreover, while algorithms aid many Americans in their everyday lives, to advance these algorithms in a manner that benefits all of society, algorithms need to be tested and designed in ways that do not discriminate against individuals unintentionally. For instance, a report has shown data can be used in ways that disadvantages vulnerable communities and targets people of color, frequently with regard to eligibility for essential products and services such as home loans.[22] Some companies have voluntarily created impact assessments to test, measure, and better understand how their algorithms work when deployed in the real world. However, many large companies, including social media, continue to deploy algorithms that may pose a consequential risk to many Americans, including but not limited to risks based on race, color, religion, national origin, sex, disability status, and political party registration status. As such, it is important that these large companies examine and better work to prevent such algorithms from causing harm to users.

Data security is also essential to protect consumers. The United States has recently seen a dramatic increase in ransomware attacks, from both state-sponsored and rogue international actors.[23] In light of these attacks by bad actors, legislation must also require businesses to ensure competent data security practices and examine how to design and implement reasonable policies for how they collect, process, and transfer individuals' information across borders. Given some of these intrusions have been associated with certain foreign actors, it is important that legislation also requires Americans to be notified when their data is accessible by China, Russia, North Korea, and Iran. In examining different ways to increase privacy protections, businesses may incorporate emerging technologies into every level of their data security practices like blockchain technology, which uses mechanisms such as decentralized identities and zero-knowledge proofs that enable information to be shared in ways that maintain the privacy of individuals while allowing more individual ownership over their data, as well as artificial intelligence.

American consumers overwhelmingly support federal privacy and data security legislation.[24] Over half of American adults now say they have decided not to use a product or service due to worries over the use of their data.[25] According to one recent poll examining provisions of H.R. 8152, 87 percent of respondents supported banning the sale of individual data to third parties without explicit consent, 86 percent supported requiring that companies minimize the data they collect from individuals, 86 percent supported increasing online data privacy protections for children under 17, and

---

[21] *The Dangerous Experiment on Teen Girls*, The Atlantic (Nov. 21, 2021).

[22] *See,* e.g., *Disparity in Home Lending Costs Minorities Millions, Research Finds*, CBS News (Nov. 15, 2019).

[23] See generally, *Treasury Sanctions IRGC—Affiliated Cyber Actions for Roles in Ransomware Activity*, U.S. Department of Treasury (Sept. 14, 2022), and, 2021 Trends Show Increase Globalized Threat of Ransomware, Cybersecurity & Infrastructure Security Agency (Feb. 10, 2022).

[24] *See,* e.g., *Voters Overwhelmingly Back Major Provisions of Proposed Federal Data Privacy Law*, Morning Consult (June 15, 2022).

[25] Pew Research Center, *Half of Americans Have Decided Not to Use a Product or Service Because of Privacy Concerns* (Apr. 14, 2020) (www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/).

82 percent supported a right for individuals to bring lawsuits if their data privacy is violated.[26]

III. COMMITTEE HEARINGS

For the purposes of section 3(c) of rule XIII of the Rules of the House of Representatives, the following hearings were used to develop or consider H.R. 8152:

The Subcommittee on Digital Commerce and Consumer Protection held an information hearing on November 1, 2017. The hearing was entitled, "Securing Consumers' Credit Data in the Age of Digital Commerce." The Subcommittee received testimony from:

- Francis Creighton, President and CEO, Consumer Data Industry Association;
- James Norton, Adjunct Lecturer, Johns Hopkins University Zanvyll Krieger School of Arts and Sciences;
- Anne P. Fortney, Esq., Partner Emeritus, Hudson Cook; and
- Bruce Schneier, Adjunct Lecturer in Public Policy, Harvard.

The Subcommittee on Digital Commerce and Consumer Protection held an informational hearing on June 14, 2018. The hearing was entitled, "Understanding the Digital Advertising Ecosystem." The Subcommittee received testimony from:

- Dr. Howard Beales, Professor of Strategic Management and Public Policy, George Washington University;
- Rachel Glasser, Global Chief Privacy Officer, Wunderman;
- Michael Zaneis, President and CEO, Trustworthy Accountability Group; and
- Justin Brookman, Director, Privacy and Technology Policy, Consumers Union.

The Subcommittee on Digital Commerce and Consumer Protection held an informational hearing on Wednesday, July 18, 2018. The hearing was entitled, "Oversight of the Federal Trade Commission." The Subcommittee received testimony from:

- The Honorable Joseph Simons, Chairman, Federal Trade Commission
- The Honorable Maureen Ohlhausen, Commissioner, Federal Trade Commission;
- The Honorable Noah Phillips, Commissioner, Federal Trade Commission;
- The Honorable Rohit Chopra, Commissioner, Federal Trade Commission; and,
- The Honorable Rebecca Slaughter, Commissioner, Federal Trade Commission.

The Subcommittee on Consumer Protection and Commerce held an informational hearing on February 26, 2019. The hearing was entitled, "Protecting Consumer Privacy in the Era of Big Data." The Subcommittee received testimony from:

- Roslyn Layton, Ph.D., Visiting Scholar, American Enterprise Institute;
- David Grimaldi, Executive Vice President for Public Policy, IAB;

[26] *Id.*

- Denise Zheng, Vice President, Technology, Innovation, Business Roundtable;
- Brandi Collins, Senior Campaign Director, Media, Democracy & Economic Justice, Color of Change; and
- Nuala O'Connor, President and CEO, Center for Democracy & Technology.

The Subcommittee on Consumer Protection and Commerce held an informational hearing on January 8, 2020. The hearing was entitled, "Americans at Risk: Manipulation and Deception in the Digital Age." The Subcommittee received testimony from:

- Monika Bickert, Head of Product Policy and Counterterrorism, Facebook;
- Joan Donovan, Ph.D., Research Director of the Technology and Social Change Project, Shorenstein Center on Media, Politics, and Public Policy, Harvard Kennedy School;
- Tristan Harris, Executive Director, Center for Humane Technology; and
- Justin (Gus) Hurwitz, Associate Professor of Law, Director of the NU Governance and Technology Center, University of Nebraska College of Law, Director of Law & Economics Programs, International Center for Law & Economics.

The Subcommittee on Consumer Protection and Commerce held an informational hearing on March 11, 2021. The hearing was entitled, "Kids Online During COVID: Child Safety in an Increasingly Digital Age." The Subcommittee received testimony from:

- Ariel Fox Johnson, Senior Counsel, Global Policy, Common Sense Media;
- Dr. Nusheen Ameenuddin, Chair, Council on Communications and Media, American Academy of Pediatrics; and
- Corey A. DeAngelis, Director of School Choice, Reason Foundation, Adjunct Scholar, Cato Institute, Executive Director, Educational Freedom Institute.

The Subcommittee on Consumer Protection and Commerce held a legislative hearing on July 28, 2021. The hearing was entitled "Transforming the FTC: Legislation to Modernize Consumer Protection." The Subcommittee received testimony from:

- The Honorable Lina Khan, Chair, Federal Trade Commission;
- The Honorable Noah Joshua Phillips, Commissioner, Federal Trade Commission;
- The Honorable Rohit Chopra, Commissioner, Federal Trade Commission;
- The Honorable Rebecca K. Slaughter, Commissioner, Federal Trade Commission;
- The Honorable Christine S. Wilson, Commissioner, Federal Trade Commission;
- David Vladeck, Professor of Law, Georgetown University Law Center;
- Sally Greenberg, Executive Director, National Consumers League; and
- Graham Dufault, Senior Director for Public Policy, ACT The App Association.

The Subcommittee on Consumer Protection and Commerce held a legislative hearing on June 14, 2022. The hearing was entitled, "Protecting America's Consumers: Bipartisan Legislation to

Strengthen Data Privacy and Security." The Subcommittee received testimony from the following witnesses:

- Caitriona Fitzgerald, Deputy Director, Electronic Privacy Information Center
- David Brody, Managing Attorney, Digital Justice Initiative, Lawyers' Committee for Civil Rights Under Law;
- Bertram Lee, Senior Policy Counsel, Data Decision Making and Artificial Intelligence, Future of Privacy Forum;
- Jolina Cuaresma, Senior Counsel, Privacy & Technology Policy, Common Sense Media;
- John Miller, Senior Vice President of Policy and General Counsel, Information Technology Industry Council;
- Graham Dufault, Senior Director for Public Policy, ACT The App Association;
- Doug Kantor, General Counsel, National Association of Convenience Stores; and
- The Honorable Maureen K. Ohlhausen, Co-Chair, 21st Century Privacy Coalition.

IV. COMMITTEE CONSIDERATION

H.R. 8152, the "American Data Privacy and Protection Act", was introduced on June 21, 2022, by Representatives Pallone (D–NJ), Rodgers (R–WA), Schakowsky (D–IL), and Bilirakis (R–FL) and was referred to the Committee on Energy and Commerce. Subsequently, on June 22, 2021, the bill was referred to the Subcommittee on Consumer Protection and Commerce. A legislative hearing was held on June 14, 2022.

On June 23, 2022, the Subcommittee on Consumer Protection and Commerce met in open markup session, pursuant to notice, to consider H.R. 8152 and seven other bills. During consideration of the bill, an amendment in the nature of a substitute (AINS), offered by Representative Pallone, was agreed to by a voice vote. Four amendments offered during consideration of the bill were withdrawn. Upon conclusion of consideration of the bill, the Subcommittee on Consumer Protection and Commerce agreed to report the bill favorably to the full Committee, amended, by a voice vote.

On July 20, 2022, the full Committee met in open markup session, pursuant to notice, to consider H.R. 8152 and five other bills. During consideration of the bill, an AINS, offered by Representative Pallone, was agreed to by a voice vote. An amendment to the AINS, offered by Representative Eshoo (D–CA), was not agreed to by a roll call vote of 8 yeas to 48 nays. Six amendments to the AINS were agreed to by a voice vote. Four other amendments to the AINS offered during consideration of the bill were withdrawn. Upon conclusion of consideration of the bill, the full Committee agreed to a motion on final passage offered by Representative Pallone, Chairman of the Committee, to order H.R. 8152 reported favorably to the House, amended, by a roll call vote of 53 yeas to 2 nays.

V. COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list each record vote on the motion to report legislation and amendments thereto. The Committee advises that there was two record votes taken on H.R. 8152, including

a motion by Mr. Pallone ordering H.R. 8152 favorably reported to the House, amended. The motion on final passage of the bill was approved by a record vote of 53 yeas to 2 nays. The following are the record votes taken during Committee consideration, including the names of those members voting for and against:

Committee on Energy and Commerce
117th Congress

Full Committee
(ratio: 32-26)
ROLL CALL VOTE #136

Bill: **H.R. 8152**, the "American Data Privacy and Protection Act"

Vote: An amendment (ESHOO_104) to the AINS by Ms. Eshoo of California, No. 1g

Disposition: **NOT AGREED TO** by a roll call vote of 8 yeas to 48 nays

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Mr. Pallone		X		Mrs. Rodgers		X	
Mr. Rush		X		Mr. Upton		X	
Ms. Eshoo	X			Mr. Burgess		X	
Ms. DeGette		X		Mr. Scalise			
Mr. Doyle		X		Mr. Latta		X	
Ms. Schakowsky		X		Mr. Guthrie		X	
Mr. Butterfield		X		Mr. McKinley		X	
Ms. Matsui	X			Mr. Kinzinger			
Ms. Castor		X		Mr. Griffith		X	
Mr. Sarbanes		X		Mr. Bilirakis		X	
Mr. McNerney	X			Mr. Johnson		X	
Mr. Welch	X			Mr. Long		X	
Mr. Tonko		X		Mr. Bucshon		X	
Ms. Clarke		X		Mr. Mullin		X	
Mr. Schrader		X		Mr. Hudson		X	
Mr. Cárdenas	X			Mr. Walberg		X	
Mr. Ruiz	X			Mr. Carter		X	
Mr. Peters	X			Mr. Duncan		X	
Mrs. Dingell		X		Mr. Palmer		X	
Mr. Veasey		X		Mr. Dunn		X	
Ms. Kuster		X		Mr. Curtis		X	
Ms. Kelly		X		Ms. Lesko		X	
Ms. Barragán	X			Mr. Pence		X	
Mr. McEachin		X		Mr. Crenshaw		X	
Ms. Blunt Rochester		X		Mr. Joyce		X	
Mr. Soto		X		Mr. Armstrong		X	
Mr. O'Halleran		X					
Ms. Rice		X					
Ms. Craig		X					
Ms. Schrier		X					
Ms. Trahan		X					
Ms. Fletcher		X					

07/20/22

Committee on Energy and Commerce
117th Congress

Full Committee
(ratio: 32-26)
ROLL CALL VOTE #137

Bill: **H.R. 8152**, the "American Data Privacy and Protection Act"

Vote: Final Passage

Disposition: **AGREED TO** by a roll call vote of 53 yeas to 2 nays

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Mr. Pallone	X			Mrs. Rodgers	X		
Mr. Rush	X			Mr. Upton	X		
Ms. Eshoo		X		Mr. Burgess	X		
Ms. DeGette	X			Mr. Scalise			
Mr. Doyle	X			Mr. Latta	X		
Ms. Schakowsky	X			Mr. Guthrie	X		
Mr. Butterfield	X			Mr. McKinley	X		
Ms. Matsui	X			Mr. Kinzinger			
Ms. Castor	X			Mr. Griffith	X		
Mr. Sarbanes	X			Mr. Bilirakis	X		
Mr. McNerney	X			Mr. Johnson	X		
Mr. Welch	X			Mr. Long	X		
Mr. Tonko	X			Mr. Bucshon	X		
Ms. Clarke	X			Mr. Mullin	X		
Mr. Schrader	X			Mr. Hudson	X		
Mr. Cárdenas	X			Mr. Walberg	X		
Mr. Ruiz	X			Mr. Carter	X		
Mr. Peters	X			Mr. Duncan	X		
Mrs. Dingell	X			Mr. Palmer	X		
Mr. Veasey	X			Mr. Dunn	X		
Ms. Kuster	X			Mr. Curtis	X		
Ms. Kelly	X			Ms. Lesko	X		
Ms. Barragán		X		Mr. Pence	X		
Mr. McEachin	X			Mr. Crenshaw	X		
Ms. Blunt Rochester	X			Mr. Joyce	X		
Mr. Soto	X			Mr. Armstrong	X		
Mr. O'Halleran	X						
Ms. Rice	X						
Ms. Craig							
Ms. Schrier	X						
Ms. Trahan	X						
Ms. Fletcher	X						

07/20/22

VI. OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII and clause 2(b)(1) of rule X of the Rules of the House of Representatives, the oversight findings and recommendations of the Committee are reflected in the descriptive portion of the report.

VII. NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

Pursuant to 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

The Committee has requested but not received from the Director of the Congressional Budget Office a statement as to whether this bill contains any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures.

VIII. FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

IX. STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the general performance goal or objective of this legislation is to establish a preemptive national consumer privacy and data security framework to protect consumer data by providing individual rights related to their personal data, imposing obligations on covered entities and service providers with respect to the collection, processing, and transfer of such data, prohibiting discrimination in providing goods and services using personal information, and creating federal, state, and individual enforcement mechanisms.

X. DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of rule XIII, no provision of H.R. 8152 is known to be duplicative of another Federal program, including any program that was included in a report to Congress pursuant to section 21 of Public Law 111–139 or the most recent Catalog of Federal Domestic Assistance.

XI. COMMITTEE COST ESTIMATE

Pursuant to clause 3(d)(1) of rule XIII, the Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

XII. EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

Pursuant to clause 9(e), 9(f), and 9(g) of rule XXI, the Committee finds that H.R. 8152 contains no earmarks, limited tax benefits, or limited tariff benefits.

XIII. ADVISORY COMMITTEE STATEMENT

No advisory committee within the meaning of section 5(b) of the Federal Advisory Committee Act was created by this legislation.

XIV. APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

XV. SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title; table of contents

This section designates that the short title may be cited as the "American Data Privacy and Protection Act" and provides a table of contents.

Sec. 2. Definitions

This section defines terms used in the Act. Key definitions are summarized below.

Subsection (9) defines "covered entity" to include any entity that collects, processes, or transfers covered data and is subject to the jurisdiction of the FTC, including nonprofits, and telecommunications common carriers. Government entities, service providers, and any congressionally designated nonprofit, national resource center, and clearinghouse to assist the public on missing and exploited child issues are expressly excluded.

Subsection (29) defines "service providers" as persons or entities that collect, process, or transfer covered data on behalf of and at the direction of a covered entity or government entity and receives covered data from or on behalf of such an entity. This covered data is defined in subsection (3) as "service provider data" and any service provider that receives service provider data from another service provider is treated as a service provider under the Act.

Subsection (36) defines "third-party collecting entities" as a subset of covered entities that for the prior 12-month period derived more than 50 percent of all revenue from or obtained revenue from processing or transferring the covered data of more than five million individuals that the covered entity did not collect directly from the individuals linked or linkable to the covered data. The extent to which an entity is acting as a service provider or is processing employee data (defined in subsection 8(c)) is not included in determining whether a covered entity is a third-party collecting entity.

Subsection (21) defines "large data holders" as covered entities or service providers that in the most recent calendar year had: (i) gross revenues of $250 million or more; and (ii) collected, processed, or transferred covered data of over five million individuals or devices and the sensitive covered data of 200,000 individuals/devices

in the most recent calendar year, excluding log-in information, phone numbers, and email addresses. Revenue for purposes of this definition with respect to nonprofit entities is defined as total gross receipts received in any form from all sources.

Subsection (35) defines "third party" as any person, including a covered entity, that collects, processes, or transfers covered data it did not collect directly from the individual to whom the data pertains and is not a service provider with respect to such data. Third parties do not include entities related by common ownership or control as defined in subsection (6) where a reasonable individual would expect the entities to share information.

Subsection (8) defines "covered data" as information, alone or in combination with other information, identifying, linked, or reasonably linkable to an individual or device linkable to an individual. This may include derived data (defined in subsection (13)) and unique persistent identifiers (defined in subsection (39)) but does not include de-identified data (defined in subsection (12)), employee data (defined in subsection (8)(c)), or publicly available information (defined in subsection (27)). "Employee" is defined in subsection (15).

Subsection (14) defines "device" as any electronic equipment capable of collecting, processing, or transferring covered data that is used by individuals.

Subsection (19) defines "individual" as any natural person residing in the United States. Subsection (11) defines "covered minor" as any individual under the age of 17.

Subsection (28) defines "sensitive covered data" as a subset of covered data categories that include: any information related to covered minors; government-issued identifiers not required to be displayed in public such as social security and passport numbers; past, present, and future health, diagnosis, disability, or treatment information; financial account, debit card, and credit card numbers along with any access code, password, or credentials; biometric information (defined in subsection (3)); genetic information (defined in subsection (18)); past or present precise geolocation information (defined in subsection (24)); private communications such as voicemail, email, text or information identifying parties to communications; any account or device log-in credentials; information revealing race, color, ethnicity, religion, or union membership status, information revealing sexual behavior that violates an individual's reasonable expectations on disclosure; information revealing online activities over time and across third party websites or online services; calendar, address book, phone, text, photos, audio and video recordings maintained for private use on a device; photos or videos of naked or undergarment-clad private areas; and information revealing video content requested by individuals using consumer-generated TV, cable, or streaming media services.

Any other covered data collected, processed, or transferred for the purpose of identifying sensitive covered data is also considered sensitive. The FTC is granted rulemaking authority under the Administrative Procedure Act (APA) to specify additional categories of covered data within the sensitive covered data definition where those categories require similar protection as a result of new methods for collecting or processing covered data.

Subsection (4) defines "collect" to mean acquiring covered data by any means.

Subsection (25) defines "process"" to mean conducting or directing any operation or set of operations performed on or otherwise handling covered data.

Subsection (38) defines "transfer" to mean disclosing, making available, or licensing covered data by any means or in any way.

Subsection (34) defines "targeted advertising" as presenting to an individual, individuals, or device(s) identified by a unique identifier an online advertisement that is selected based on known or predicted preferences, characteristics, or interests. It does not include responses to an individual's specific request for information; contextual advertising when an advertisement is displayed based on the content of a webpage or online service; or processing of data solely used for measuring or reporting advertising metrics.

Subsection (17) defines "first party advertising or marketing" as such activities conducted by the first party entity that operates a consumer-facing website or physical location either (i) through direct communication with an individual; or (ii) entirely within the first-party context.

Subsection (1) defines "affirmative express consent" to provide the conditions necessary for covered entities and service providers to obtain consent as required under the Act, including prohibiting pretextual consent, preventing silence or use of a product or service as consent, requiring reasonably accessible means to consent, and prohibiting manipulative designs or materially misleading representations to obtain consent.

Subsection (7) defines "covered algorithm" as a computational process that uses machine learning, natural language processing, artificial intelligence techniques, or other computational processing techniques of similar or greater complexity, that makes a decision or facilitates human decision-making with respect to covered data.

Subsection (20) defines "knowledge" using a tiered approach in regard to covered minors based on the entity involved. A knew or should have known standard applies to "covered high-impact social media companies" with platforms primarily used by individuals for user-generated content, at least $3 billion in annual revenue, and 300 million monthly active users for 3 of the prior 12 months; a knew or acted in "willful disregard" of an individual's age standard applies to all other large data holders, including service providers; and an actual knowledge standard applies to all other covered entities and service providers.

Subsection (32) defines "state privacy authority" as either the chief consumer protection officer of a state or any state consumer protection agency with expertise in data protection, including the California Privacy Protection Agency (CPPA).

TITLE I—DUTY OF LOYALTY

Sec. 101. Data minimization

Subsection (a) imposes a baseline duty on all covered entities not to collect, process, or transfer covered data beyond what is reasonably necessary and proportionate to provide a particular requested product or service or to affect a permitted purpose under subsection (b), regardless of any consent or transparency requirements.

Subsection (b) sets out 17 enumerated permissible purposes for which covered entities may collect, process, or transfer covered data. If the use of covered data does not fit one of these categories or is not covered by subsection (a) it is per se prohibited. These permissible purposes include the use of covered data to: complete transactions and routine administrative, operational, or account-servicing activity such as billing, delivery, storage, and accounting; with respect to data previously collected in accordance with the act, perform system maintenance, and related internal functions using covered data already lawfully collected under the Act, develop, maintain, repair, or enhance a product or service for which such data was collected, to conduct internal research or analytics to improve a product or service, to perform inventory management or network management, protect against spam, or debug or repair errors that impair the functionality of the requested product or service; authenticate users; fulfill warranties; prevent, detect, and respond to network and physical security incidents; prevent, detect, and respond to fraud, harassment, and illegal activity capable of direct harm; comply with legal obligations and defend legal claims; prevent death or serious injury; effectuate product recalls pursuant to law; conduct public or peer-reviewed research meeting certain requirements; deliver reasonably anticipated, non-advertising communications; deliver communications at the direction of an individual; transfer assets to a third party in merger, acquisition, bankruptcy, or similar transaction after providing notice and opportunity for withdrawing prior consent; ensure data security and integrity pursuant to section 208; transfer previously collected covered data in accordance with the Act to a government entity provided it is not for consideration and pursuant to statutory authorization to prevent, detect, or protect against public safety incidents, natural disasters, or national security incidents; with respect to previously collected covered data providing first-party marketing of goods and services provided by the covered entity to individuals 17 and older; and with respect to previously collected covered data providing targeted advertising that otherwise complies with the Act.

Subsection (c) requires the FTC to issue guidance to help establish what is "reasonably necessary and proportionate" to comply with this section taking into account specific characteristics of the covered entity and its covered data activities.

Subsection (d) prohibits covered entities and service providers from engaging in deceptive advertising or marketing of any product or service.

Sec. 102. Loyalty duties

Subsection (1) prohibits collecting, processing, or transferring Social Security numbers except for credit extension, authentication, fraud prevention, paying or collecting taxes, enforcing contracts, or as required by law.

Subsection (2) requires any collection or processing of sensitive covered data to be limited to what is strictly necessary for specific products or services requested by individuals or certain permitted purposes, which do not include first-party marketing or targeted advertising purposes.

Subsection (3) prohibits the transfer of sensitive covered data to third parties except (i) with affirmative express consent; (ii) to comply with law; (iii) prevent imminent risk of death or serious injury; (iv) transferring previously collected covered data to a government entity provided it is not for consideration and pursuant to statutory authorization to prevent, detect, or protect against public safety incidents, natural disasters, or national security incidents; (v) transferring passwords for use across sites or accounts; (vi) transferring genetic information for requested medical diagnosis or treatment or research; or (vii) transferring assets as described in section 101(b)(13).

Subsection (4) specifies that providers of broadcast television services, cable services, satellite services, streaming media services, or other non-consumer-generated video programming services may only transfer covered data revealing content or services requested by users with affirmative express consent or pursuant to a permissible purpose in section 101(b)(1)–(15).

Sec. 103. Privacy by design

This section requires covered entities and service providers to implement reasonable policies, practices, and procedures for collecting, processing, and transferring covered data including training, risk mitigation (including substantial privacy risks), and compliance. These should correspond to the entity's size, complexity, activities related to covered data, the types and amount of covered data the entity engages with, and the cost of implementation compared to the risks posed. Privacy by design must also take into account the particular privacy risks related to covered minors with heightened requirements for entities not meeting the criteria for entities defined in section 209.

The FTC must issue guidance on reasonable policies, practices, and procedures under this section within one year of enactment.

Sec. 104. Loyalty to individuals with respect to pricing

This section prohibits covered entities from retaliating against an individual for exercising any rights guaranteed by the Act, including denying goods or services, discriminating in the price or rate for goods or services, or providing a different level of quality of goods or services.

This prohibition does not prevent covered entities from differentiating the price of or levels of services based on an individual providing financial information necessarily collected and used for payment when an individual specifically requests a product. Covered entities are also not prevented from offering bona fide loyalty programs that provide rewards, premium features, discounts, or club card programs in exchange for continued business on a voluntary basis. Covered entities may also charge different prices based on individuals exercising deletion rights under section 203(a)(3), provide financial incentives for market research participation, and decline to provide products or services where certain collecting or processing of covered data is strictly necessary.

TITLE II—CONSUMER DATA RIGHTS

Sec. 201. Consumer awareness

Within 90 days of enactment, the FTC must publish a public web page describing all provisions of the Act in plain language, listed separately to help advise individuals and covered entities of their rights and obligations under the Act. The web page must be updated for changes in law. The information must be published in the ten languages with the most speakers in the United States.

Sec. 202. Transparency

Covered entities must provide individuals with privacy policies detailing their data collection, processing, and transfer activities in a readily available and understandable manner.

Covered entities and service providers must have privacy policies that include contact information, the affiliates of the covered entity that it transfers covered data to, and the purposes for each category of covered data the entity collects, processes, and transfers. Covered entities and service providers must specify the third-party collecting entities to whom they transfer covered data and for what purposes. Privacy policies must be provided in every covered language the entity provides or carries out products/services under the policy and in an accessible manner for individuals with disabilities.

Privacy policies must also state how individuals may exercise their rights under the Act and how long the entity intends to retain covered data. Privacy policies must be provided in all languages in which covered entities conduct business related to the covered data. Any material changes to a covered entity's privacy policy requires the covered entity to notify individuals and provide an opportunity to withdraw consent before further processing the covered data of those individuals. Covered entities and service providers must specify whether any covered data they handle is accessible by China, Russia, Iran, or North Korea.

Finally, large data holders must keep a log of publicly available material changes to their policies for the prior ten years after enactment of the Act and provide short-form notices of their covered data practices pursuant to minimum requirements established in FTC regulations issued in accordance with the Administrative Procedure Act (APA).

Sec. 203. Individual data ownership and control

Subsection (a) establishes individual rights to access, correct, delete, and port covered data that pertains to them. The right to access includes obtaining covered data possessed by the covered entity within 24 months preceding the request in a human-readable and downloadable format that individuals may understand without expertise; the categories of any other entities their data was transferred to and the names of any such third parties upon request; the categories of sources used to collect any covered data; and the purposes for transferring the data. The rights to correct and delete covered data also require covered entities to notify other entities to whom covered data was transferred of the corrected information or desire to have the covered data deleted. To the extent technologically feasible, individuals also have the right to export their

covered data in human-readable and a machine-readable, interoperable, portable format.

Subsection (b) prevents the use of dark patterns or other manipulative measures with the purpose or substantial effect of impairing individual autonomy in exercising such a decision to exercise any rights under this section.

Subsection (c) establishes staggered time limits for covered entities to comply with requests based on the size of the entity.

Subsection (d) allows for reasonable fees for the exercise of the third and subsequent exercises of each of the rights described in (a) within one 12-month period.

Subsection (e) states that covered entities are not required to comply with individual requests under this section where they are unable to verify the identity of the individual making the request; reasonably believe the request would interfere with a contract between the covered entity and another individual; determine that completing the request would require access to or correction of another individual's sensitive covered data; reasonably believe the exercise of the request would require the entity to engage in an unfair or deceptive act or practice; or reasonably believe the request would further fraud, support criminal activity, or the exercise of the right presents a data security threat. Covered entities may seek additional information for verification purposes. These individual rights are subject to covered entities rights to limited permissive exceptions for covered data use, such as complying with law enforcement or judicial proceedings. Covered entities must partially comply with requests where feasible.

Subsection (f) requires covered entities that are large data holders to annually compile metrics of requests and responses and disclose such metrics publicly.

Subsection (g) requires the FTC, not later than two years after enactment, to promulgate APA regulations as necessary to establish processes for compliance with this section, taking into consideration various characteristics of different covered entities and their activities with respect to covered data.

Subsection (h) requires covered entities facilitate individual rights requests in all covered languages and in a manner accessible to individuals with disabilities.

Sec. 204. Right to consent and object

Subsection (a) makes clear that the means to withdraw any affirmative express consent must be as easy to execute as the means to provide such consent.

Subsection (b) provides individuals with the right, subject to limited exceptions in paragraphs (1)–(15) of section 101(b), to object to the transfer of their covered data to a third party and individuals must be provided the right to opt-out of such transfers through a universal opt-out mechanism as described in section 210.

Subsection (c) provides that covered entities and service providers that directly deliver targeted advertising must, prior to engaging in such advertising and at all times thereafter, provide individuals with clear and conspicuous means to opt out, abide by any such opt-out, and allow individuals to opt-out of targeted advertising through a universal opt-out mechanism as described in section 210. Service providers and covered entities providing targeted

advertising must notify each other of the opt-out designation as applicable.

Subsection (d) prevents the use of dark patterns or other manipulative measures with the purpose or substantial effect of impairing individual autonomy in exercising such a decision to opt-out.

Sec. 205. Data protections for children and minors

Covered entities are subject to additional requirements for covered data with respect to covered minors. Subsection (a) prohibits targeted advertising to any individual that the covered entity has knowledge is a covered minor.

Subsection (b) prohibits the transfer of covered data of any individual that the covered entity has knowledge is a covered minor to third parties without affirmative express consent of the minor or a parent or guardian unless to transfer data in order to submit information relating to child victimization to law enforcement or to the nonprofit, national resource center and clearinghouse designated to provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children.

Subsection (c) establishes a Youth Privacy and Marketing Division within the privacy bureau at the FTC established under section 401, which shall be responsible for addressing privacy and marketing concerns with respect to children and minors. The division must submit annual reports to Congress and hire staff that includes experts in youth development, data protection, digital advertising, and data analytics.

Subsection (d) requires the FTC Inspector General to submit a report to Congress every two years analyzing the fairness and effectiveness of the safe harbor provisions in COPPA. These reports must be published on the FTC web site.

Sec. 206. Third-party collecting entities

Subsection (a) requires that all third-party collecting entities place a clear and conspicuous, reasonably accessible notice on their web site and/or mobile application informing individuals they are a third-party collecting entity using language specified by FTC regulations. The FTC must promulgate such regulations in accordance with APA and require a link to the third-party collecting entity registry described under subsection (b).

Subsection (b) directs the FTC to establish a third-party collecting registry. Third-party collecting entities that process covered data of more than 5,000 individuals or devices must annually register with the FTC. Registration includes paying a $100 fee, providing information about the third-party collecting entity's activities, providing contact information, and creating a link to a website where individuals may exercise their audit rights under this section.

The FTC must establish and maintain an online, public, searchable registry of registered third-party collecting entities that allows individuals to look up information on third-party collecting entities, links to and contact information of the third-party collecting entities, and a link and mechanism by which individuals may submit a single request to all registered third-party collecting entities to,

within 30 days, have all covered data about them deleted and ensure no further covered data collection related to them will take place. The FTC must establish universal opt-out mechanism(s) under section 210 to effectuate this right.

Subsection (c) imposes penalties on third-party collecting entities for failing to register or provide the notice required by this section, which include civil fines of $100 per day (up to $10,000 per year) and any unpaid registration fees. Such penalties come in addition to other enforcement and remedies in the Act and do not limit additional enforcement.

Sec. 207. Civil rights and algorithms

Subsection (a) provides that covered entities and service providers may not collect, process, or transfer covered data in a manner that discriminates or otherwise makes unavailable the equal enjoyment of goods and services on the basis of race, color, religion, national origin, sex, or disability in line with current Supreme Court precedent in prohibiting discrimination on the basis of protected classes. This does not prevent covered entities from diversifying an applicant, participant, or customer pool.

Subsection (b) states that, as applicable, the FTC is required to transmit any information it obtains regarding potential discriminatory uses of covered data to federal executive agencies with authority to initiate proceedings related to such a violation. The FTC must submit annual reports to Congress on the information it sends to these agencies under this section and how that information relates to federal civil rights laws.

Subsection (c) requires large data holders that use covered algorithms to assess such algorithms that are used in a manner that poses a consequential risk of harm to an individual or group of individuals and submit annual algorithmic impact assessments to the FTC. These assessments must in part describe steps the entity has taken or will take to mitigate potential harms from covered algorithms, including any harms specifically related to covered minors or substantial privacy risks. These assessments must also seek to mitigate algorithmic harms related to advertising for housing, education, employment, healthcare, insurance, or credit, access to or restrictions on places of public accommodation, and any disparate impact on the basis of an individual's race, color, religion, national origin, sex, or disability status, or a disparate impact on the basis of individuals' political party registration status.

Algorithmic evaluations are also required at the design phase of a covered algorithm that is designed at least in part in furtherance of a consequential decision, including any training data that is used to develop such algorithm. The FTC may not use any information received solely through these required submissions for any purpose outside enforcing this act and consent orders. Covered entities may redact and segregate any trade secrets or other confidential or proprietary information from public disclosure and the Commission shall abide by their obligations in regard to such information.

The FTC must publish guidance regarding compliance with this section. The FTC is also granted rulemaking authority in accordance with APA to promulgate regulations establishing processes for submitting algorithmic impact assessments and excluding any cov-

ered algorithms it deems to present minimal consequential risks of harm to individuals.

Finally, the FTC must, in consultation with the Department of Commerce (DOC), conduct a study using its authority under section 6(b) of the FTC Act to review the algorithmic impact assessments received under this section and submit a report to Congress containing the results of the study. Additional reports are required three years after the initial submission as well as whenever the FTC deems it necessary.

Sec. 208. Data security and protection of covered data

Subsection (a) requires covered entities and service providers to implement and maintain data security practices and procedures that protect and secure covered data against unauthorized use and acquisition. In determining whether such protections are reasonable, the FTC, state enforcement authorities, and federal courts must consider the entity's size, complexity, activities related to covered data, the types and amount of covered data the entity engages with, the current state of the art in administrative, technical, and physical safeguards for protecting covered data, and the cost of available tools.

Subsection (b) provides specific requirements certain covered entities and service providers must meet in order to assess vulnerabilities, take preventive and corrective action, evaluate their systems, and for the retention and disposal of covered data. Such covered entities and service providers must also provide training to all employees with access to covered data and designate an officer or employee to maintain and implement their data security practices.

The FTC may promulgate regulations in accordance with APA to establish processes for compliance with this section and shall consult with the National Institute of Standards and Technology when doing so.

Sec. 209. Small business protections

This section sets eligibility criteria and provides exemptions for certain entities.

Subsection (a) states that any covered entity or service that meets the requirements of subsection (b) will be: (i) exempt from the data portability requirements in section 203(a)(4), the data security requirements in section 208(b) with the exception of the data retention and disposal provisions in section 208(b)(4), and section 301(c) requirements; and (ii) may choose to delete, rather than correct, an individual's covered data upon receiving a verified request in section 203(a)(2).

Subsection (b) establishes that covered entities or service providers that for the prior three years (or the entity's existence if less than three years): (i) earned average gross annual revenues of $41 million or less; (ii) did not collect or process the covered data of 200,000 individuals in a year on average (except for processing payments and deleting covered data for requested products/services after 90 days, except when necessary to investigate fraud or as consistent with a covered entity's return policy); and (iii) did not derive more than half their revenue from transferring covered data meet the eligibility requirements.

Subsection (c) defines revenue for purposes of this section with respect to nonprofit entities as total gross receipts received in any form from all sources.

Sec. 210. Unified opt-out mechanisms

Subsection (a) provides that following public notice and opportunity for comment, within 18 months of enactment of the Act the FTC must establish or recognize one or more acceptable, privacy-protective, centralized opt-out mechanisms to allow individuals to exercise their rights to opt-out of covered data transfers in section 204(b), targeted advertising in section 204(c) (except for first-party marketing to individuals 17 and older), and the single request to all registered third-party collecting entities to have all covered data about them deleted and to refrain from further covered data collection as provided in section 206(b)(3)(C). Such mechanisms may include global privacy signals such as browser or device privacy settings, other tools offered by covered entities or service providers, or registries of identifiers.

Subsection (b) sets out six criteria the opt-out mechanisms must meet that will ensure the mechanisms inform individuals of their choices, represent freely given choices, are easy to use, allow for authentication of requests, are made in any covered language that the covered entity provides products or services subject to the opt-out, and be reasonably accessible to those with disabilities.

TITLE III—CORPORATE ACCOUNTABILITY

Sec. 301. Executive responsibility

Subsection (a) requires that an executive officer at all large data holders annually certify that their company maintains reasonable internal controls and reporting structures for compliance with the Act in the manner specified by the FTC through APA rulemaking.

Subsection (b) requires this certification must be based on a review conducted by the certifying officers within 90 days of submission.

Subsection (c) requires all covered entities or service providers with more than 15 employees to designate one or more privacy and data security officers who must implement privacy and data security programs and ensure ongoing compliance with the Act. Large data holders must also designate at least one of these officers as the privacy protection officer to report directly to the entity's highest official. That officer is responsible for establishing processes, conducting regular comprehensive audits, developing training and education programs for employees, maintaining records, and serving as the point of contact with enforcement authorities as related to the privacy and security requirements of the Act.

Subsection (d) requires covered entities that are large data holders to also conduct privacy impact assessments weighing the benefits of its covered data practices against the potential consequences to individual privacy on a biennial basis and have them approved by the privacy protection officer. In assessing the privacy risks, the large data holder may include reviews of the means by which technologies, including blockchain and distributed ledger technologies and other emerging technologies, are used to secure personal information.

Subsection (e) requires all covered entities that are neither large data holders nor meet the requirements of section 209 to conduct privacy impact assessments that weigh the benefits of the covered entity's collecting, processing, and transfer practices that may cause a substantial privacy risk against the potential material adverse consequences of such practices to individual privacy.

Sec. 302. Service providers and third parties

Subsection (a) outlines the obligations of service providers. In so far as a person acts as a service provider, it may only collect, process, or transfer service provider data for the purposes directed by the covered entity or government entity it received the data from as set out in the contract required under subsection (b). Service providers may not collect, process, or transfer service provider data if it has actual knowledge the covered entity violated the Act with respect to such data. Service providers must assist the covered entities they provide services for in fulfilling requests by individuals to exercise their rights under sections 203 and 204 of the Act by either providing appropriate technical measures or fulfilling the requests. Service providers may only engage other service providers as subcontractors after providing the relevant covered entity with notice and pursuant to a written contract extending all responsibilities to the subcontractor. Service providers must also make certain information available to covered entities, delete, or return covered data as specified, abide by data protection and confidentiality safeguards consistent with section 208, and allow for reasonable assessments by the covered entity.

Subsection (b) provides that contracts between covered entities and service providers must set out clear instructions and cannot relieve any party of any requirement or liability imposed under the Act. Combining service provider data with other covered data is prohibited except for limited exceptions. Service providers must retain copies of prior contracts with covered entities required under this section.

Subsection (c) makes clear that determining whether a person is acting as a covered entity or service provider with respect to covered data is a fact-based, contextual determination and sets out how liability may be apportioned for violations of the Act.

Subsection (d) establishes that third parties cannot process third party data beyond the processing purpose for which a covered entity made a disclosure under section 202 and in the case of non-sensitive data, the processing purpose for which the covered entity made a disclosure pursuant to section 202(b)(4).

Subsection (e) establishes that covered entities and service providers must conduct reasonable due diligence in selecting service providers and deciding to transfer covered data to third parties. The FTC must issue guidance to help entities comply with this section, including to help alleviate potentially unreasonable compliance burdens on small entities.

Sec. 303. Technical compliance programs

Subsection (a) provides that within three years of enactment, the FTC must promulgate regulations under the APA to establish processes for covered entities to submit technical compliance programs for approval.

Subsection (b) outlines that such programs are to be specific to particular technologies, products, services, or methods used by a covered entity to collect, process, or transfer covered data. Such programs will establish compliance guidelines that meet or exceed the Act's requirements and be publicly available to individuals whose data is processed by participating entities.

Subsection (c) requires that any application for approval or amendment of existing programs will be made public by the FTC along with a request for public comment within 90 days.

Subsection (d) provides the opportunity for any final action by the FTC on a request for approval, amendment, or appeal of a technical compliance program to be appealed to a Federal district court of the United States.

Subsection (e) requires that the FTC and state enforcement authorities must consider a covered entity's history of compliance with any approved program before bringing an enforcement action against that entity and courts in private litigation must consider such compliance when determining liability or penalty. However, compliance with a program under section 303 shall not impact any burden of proof or weight given to evidence in any enforcement or judicial proceeding.

Nothing in this section shall provide any individual with any right to seek discovery of any non-public FTC deliberations or activities or impose any pleading requirement on the FTC.

Sec. 304. Commission approved guidelines

Non-third-party collecting entities that meet the criteria in section 209 are eligible to participate in FTC approved compliance guidelines for handling covered data. Applications for approval must include how the guidelines will meet or exceed the Act's requirements, the entities, or activities the guidelines intend to cover, any covered entities known at the time of submission who want to participate, and a description of how entities will be independently assessed for compliance. Compliance with any approved guidelines must be assessed by an independent organization not associated with any covered entity participant and that organization must be identified in the application for approval.

Any application for approval will be made public by the FTC along with a request for public comment within 90 days. The FTC has one year from receipt to approve a submission. Applications must include how regular review, validation, and enforcement by the independent organization administering the guidelines will take place, including any referral mechanism to the FTC, if applicable. Material changes to the guidelines must also be submitted for approval, which the FTC must respond to in approve or deny within one year.

The FTC may withdraw approval at any time if it believes the guidelines no longer meet or exceed the Act's requirements or enforcement by the independent organizing administering the guidelines is insufficient. The FTC must notify the participating covered entities its basis for doing so, beginning a 180-day timeline to cure the deficiency in the guidelines and submit the proposed cure to the FTC for approval. If the FTC finds the deficiency is cured, then it may not withdraw approval of the guidelines.

An entity eligible to participate in approved guidelines remains subject to enforcement and will be deemed in compliance with the Act if it able to illustrate compliance with the guidelines.

Sec. 305. Digital content forgeries

This section requires that within a year after enactment and annually after that the Department of Commerce (DOC) must publish a report on digital content forgeries. Such reports will define, describe, and assess digital content forgeries, including the methods to identify and take countermeasures against them along with anything else determined appropriate by the Secretary of Commerce or the Secretary's designee.

TITLE IV—ENFORCEMENT, APPLICABILITY, AND MISCELLANEOUS

Sec. 401. Enforcement by the Federal Trade Commission

Subsection (a) provides that the FTC must establish a new bureau of privacy to carry out its authority under the Act that is comparable to the current Bureaus of Consumer Protection and Competition. That bureau must be fully operational within a year of enactment and include an office of business mentorship to assist covered entities with compliance as described in subsection (b).

Subsection (c) specifies that violations of the Act will be treated as violations of a rule defining an unfair or deceptive act or practice under the FTC Act, meaning the FTC may obtain civil penalties for initial and subsequent violations, among other relief. The FTC may generally enforce the Act akin to any other violation under the FTC Act, but it may not bring an action under section 5(b) of the FTC Act to stop the same conduct that it brings an enforcement against under this Act.

This section also establishes a relief fund for victims of entities violating the Act. Any relief obtained enforcing the Act under this section that cannot be provided directly to harmed individuals will be deposited there and be available to the FTC, without fiscal year limitation, to provide relief to individuals harmed by violations under the Act. To the extent money in the fund cannot be used to compensate harmed individuals, the FTC may use funds for the office of business mentorship or to engage in technological research.

Sec. 402. Enforcement by States

State Attorneys General and state privacy authorities may bring civil actions in federal court for injunctive relief, enforce compliance, to obtain damages, penalties, restitution, or other compensation, and to obtain reasonable attorney's fees and other litigation costs. The FTC retains the right to intervene upon receiving required notice from state enforcement officers and no state enforcement may occur once the FTC or its deputy has initiated an enforcement action regarding that conduct. States retain all of their existing investigatory, regulatory, and administrative powers and rights to bring enforcement actions arising under existing state law, including bringing regulatory proceedings.

Sec. 403. Enforcement by persons

Subsection (a) allows private rights of actions by individuals harmed under the Act. Starting two years after the date the Act

takes effect, persons or classes of persons may generally bring a civil action in federal court seeking compensatory damages, injunctive relief, declaratory relief, and reasonable attorney's fees and litigation costs.

Prior to initiating a civil action, individuals must notify the FTC and the attorney general of their state of residence of their intent to bring such an action; those agencies then have 60 days to determine if they wish to intervene pursuant to the Federal Rules of Civil Procedure. State intervention allows state enforcement agencies to be heard with respect to the interests of their state residents. Demands for monetary payments sent to covered entities or service providers prior to the end of this period or after one of the authorities has opted to bring an action will be considered to be made in bad faith. All demand letters must provide a statement and link to the FTC website established by section 201 of the Act that describes a covered entity's rights under the Act. Failure to properly send demand letters under subsection (d) will result in dismissal without prejudice.

The FTC's Bureau of Economics and Bureau of Privacy must conduct annual studies beginning five years after enactment regarding the impact of demand letters under the Act and report these findings to Congress.

Subsection (b) prohibits covered entities and service providers from enforcing pre-dispute arbitration agreements or joint action waivers with respect to minors. Pre-dispute arbitration agreements are also unenforceable for any claims related to gender or partner-based violence or physical harm.

Subsection (c) provides a right to cure certain violations by all covered entities and for any violation that meet the requirements for small business under section 209. When individuals advance claims of injunctive relief or claims of any relief against such entities, those entities have a right to cure the alleged deficiency. Covered entities and service providers must be provided 45 days written notice identifying specific provisions the entity allegedly violated. When an entity successfully demonstrates to a court that a cure is achieved and no further violations will occur, demands for injunctive relief may be reasonably dismissed.

Subsection (e) states that the rights in this section applies to claims alleging violations of sections 102, 104, 202, 203, 204, 205(a)–(b), 206(b)(3)(C), 207(a), 208(a), or 302 and any regulation promulgated under such sections. No private suits may be brought against a covered entity with less than $25 million in annual revenue that collects, processes, or transfers the covered data of fewer than 50,000 individuals and derives less than half its revenue from transferring covered data.

Sec. 404. Relationship to Federal and State laws

Subsection (a) provides that existing federal law and the authority of federal agencies is generally not limited except where specified in the Act. Nothing in the Act limits antitrust law in any way. Covered entities subject to and in compliance with the related data privacy and security requirements of certain specified federal laws shall be held to be in compliance with the related laws of the Act solely and exclusively to the extent that covered data is subject to

the requirements in the other laws. The FTC must issue guidance for implementation of these provisions.

Subsection (b) provides that state laws covered by the provisions of the Act are preempted, subject to a list of specified state laws to be preserved. That list of laws or provisions of law includes: generally applicable consumer protection laws; civil rights laws; employee and student privacy protections; data breach notification laws; contract and tort law; criminal laws; civil laws regarding fraud, theft, identity theft, unauthorized access to electronic devices, and unauthorized use of personal information; laws on cyberstalking, cyberbullying, nonconsensual pornography, sexual harassment, and child abuse; unrelated public sector and safety laws; provisions of laws solely addressing public records and criminal justice information; provisions of laws solely addressing bank, financial, and tax records, Social Security numbers, credit cards, credit reporting, credit repair, credit clinics, and check-cashing services; provisions of laws solely addressing facial recognition, electronic surveillance, wiretapping, and telephone monitoring; the Illinois Biometric and Genetic Information Privacy Acts; provisions of laws solely addressing unsolicited email, text messages, caller identification, and phone calls; provisions of laws solely addressing medical information, records, and HIV status or testing; provisions of laws solely addressing public health; provisions of law solely addressing the confidentiality of library records; Section 1798.150 of the California Civil Code, as amended; and laws pertaining to encryption as a means of data security. State common law rights or remedies and statutes creating remedies for civil relief are not preempted or displaced by the Act, but violations of the Act shall not be pleaded as an element of any such cause of action.

Sections 222, 338(i), and 631 of the Communications Act of 1934 and any related Federal Communications Commission (FCC) orders or regulations shall not apply to covered entities with respect to the collecting, processing, or transferring covered data under the Act and the related privacy and data security of such a covered entity will be governed exclusively by the Act except for emergency services, subsections (b) and (g) of section 222 of the Communications Act of 1934, and any obligation of an international treaty related to the exchange of traffic implemented and enforced by the FCC.

Sec. 405. Severability

This section provides that if any provision of the Act is held invalid, the remainder of the Act will remain valid to the furthest extent possible.

Sec. 406. COPPA

This section states that the Act does not relieve or change existing obligations under COPPA and that within 180 days of enactment the FTC must amend its existing COPPA rules to reference additional requirements to covered entities under the Act.

Sec. 407. Authorization of appropriations

This section authorizes the FTC to be appropriated the sums necessary to carry out the Act.

Sec. 408. Effective date

This section specifies that the Act will take effect 180 days after the date of enactment.

XVI. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

There are no changes to existing law made by the bill H.R. 8152.

○