A DRAFT OF PROPOSED LAW

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

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

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

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.

TITLE I—DUTY OF LOYALTY

Sec. 101. Data minimization.
Sec. 102. Loyalty duties.
Sec. 103. Privacy by design.
Sec. 104. Loyalty to individuals with respect to pricing.

TITLE II—CONSUMER DATA RIGHTS

Sec. 201. Consumer awareness.
Sec. 202. Transparency.
Sec. 203. Individual data ownership and control.
Sec. 204. Right to consent and object.
Sec. 205. Data protections for children and minors.
Sec. 206. Third-party collecting entities.
Sec. 207. Civil rights and algorithms.
Sec. 208. Data security and protection of covered data.
Sec. 209. Small business protections.
Sec. 210. Unified opt-out mechanisms.

TITLE III—CORPORATE ACCOUNTABILITY

Sec. 301. Executive responsibility.
Sec. 302. Service providers and third parties.
Sec. 303. Technical compliance programs.
Sec. 304. Commission approved compliance guidelines.
Sec. 305. Digital content forgeries.

TITLE IV—ENFORCEMENT, APPLICABILITY, AND MISCELLANEOUS

Sec. 401. Enforcement by the Federal Trade Commission.
Sec. 402. Enforcement by States.
Sec. 403. Enforcement by persons.
Sec. 404. Relationship to Federal and State laws.
Sec. 405. Severability.
Sec. 406. COPPA.
Sec. 407. Authorization of appropriations.
Sec. 408. Effective date.

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

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

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

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

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

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

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

(xii) Information revealing the video content requested or selected by an individual collected by a covered entity that is not a provider of a service described in section 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 exclusive 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, except 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 information as allowable under Federal law to any Executive agency with authority to initiate enforcement actions or proceedings relating to such violation.

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

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

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

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

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

(c) COVERED ALGORITHM IMPACT AND EVALUATION.—

(1) COVERED ALGORITHM IMPACT ASSESSMENT.—

(A) IMPACT ASSESSMENT.—Notwithstanding any other provision of law, not later than 2 years after the date of enactment of this Act, and annually thereafter, a large data holder that uses a covered algorithm in a manner that poses a consequential risk of 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 assessment of the service provider's policies and technical and organizational measures in support of the obligations under this Act using an appropriate and accepted control standard or framework and assessment procedure for such assessments. 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 counter-measures 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 desist 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 respect 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.

Union Calendar No. 488

117TH CONGRESS
2D SESSION

H. R. 8152

[Report No. 117–669]
