.....

(Original Signature of Member)

117TH CONGRESS
2D SESSION

H. R. _____

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

IN THE HOUSE OF REPRESENTATIVES

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

A BILL

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 State Attorneys General.
Sec. 403. Enforcement by individuals.
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, informed, and unambiguous authorization for an act or prac-

tice, 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.

(ii) The request includes a description of the act or practice 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 for each act or practice;

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

(III) 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 shall be made in a manner readily accessible to and usable by individuals with disabilities.

(v) The request shall be made available to the public in each language in which the covered entity provides a product or service for which authorization is sought or in which the covered entity carries out any activity related to any product or service for which the covered data of the individual may be collected, processed, or transferred.

(C) EXPRESS CONSENT REQUIRED.—A covered entity shall 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 shall 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) ALGORITHM.—The term ''algorithm'' means a computational process that uses machine learning, natural language processing, artificial intelligence techniques, or other computational processing tech-

niques of similar or greater complexity that makes a decision or facilitate 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.

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

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

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

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

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

(8) COVERED 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 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, provided that such informa-

tion 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) 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, provided that such information is collected, processed, or transferred solely for purposes related to such employee's professional activities;

(iii) emergency contact information collected by an employer that relates to an employee of that employer, provided that such information is collected, processed, or transferred solely for the purpose of having an emergency contact on file for the employee; or

(iv) 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.—The term ''covered entity''—

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

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

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

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

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

(ii) a person or an entity that is collecting, processing, or transferring covered data on behalf of or a Federal, State, Tribal, territorial, or local government entity.

(10) DE-IDENTIFIED DATA.—The term ''de-identified data'' means information that does not identify and is not linked or reasonably linkable to an individual or an individual's device, regardless of whether the information is aggregated, provided that the covered entity—

(A) takes reasonable technical, administrative, and physical measures to ensure that the

information cannot, at any point, be used to re-identify any individual or device;

(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; and

(C) contractually obligates any person or entity that receives the information from the covered entity to comply with all of the provisions of this paragraph.

(11) 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.

(12) DEVICE.—The term ''device'' means any electronic equipment capable of transmitting or receiving covered data that is designed for use by one or more individuals.

(13) EMPLOYEE.—The term ''employee'' means (regardless of whether such employee is paid, unpaid, or employed on a temporary basis) an employee, director, officer, staff member, an individual working as a contractor, trainee, volunteer, or intern of an employer.

(14) EXECUTIVE AGENCY.—The ''Executive agency'' has the meaning set forth in section 105 of title 5, United States Code.

(15) 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 an individual's complete extracted or a portion of the extracted deoxyribonucleic acid (DNA); or

(B) genotypic and phenotypic information that results from analyzing the raw sequence data.

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

(17) LARGE DATA HOLDER.—The term ''large data holder'' means a covered entity or service provider that, in the most recent calendar year—

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

(B) 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; 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.

(C) EXCLUSIONS.—The term ''large data holder'' does not include any instance where the covered entity or service provider would qualify as a large data holder solely on account 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.

(D) REVENUE.—For purposes of this determining whether any covered entity or service provider is a large data holder, 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.

(18) 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.

(19) 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 an individual's decision or conduct regarding a product or service.

(20) PRECISE GEOLOCATION INFORMATION.—

(A) IN GENERAL.—The term ''precise geolocation information'' means information that reveals the past or present physical location of an individual, or device that identifies or is linked or reasonably linkable to 1 or more individuals, with sufficient precision to identify street level location information or an individual's location within a range of 1,000 feet or less.

(B) EXCLUSION.—The term ''precise geolocation information'' does not mean geolocation information identifiable solely from the visual content of an image.

(21) 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.

(22) PROCESSING PURPOSE.—The term ''processing purpose'' means a reason for which a covered entity 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 collects, processes, or transfers the covered data.

(23) PUBLICLY AVAILABLE INFORMATION.—

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

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

(ii) widely distributed media;

(iii) a website or online service made available to all members of the public, for

free or for a fee, including where all members of the public can log-in to the website or online service;

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

(v) a visual observation of an individual's physical presence in a public place by another person, 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 for purposes of section 1460 of title 18, United States Code);

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

(III) biometric information;

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

(V) genetic information; or

(VI) known nonconsensual intimate images.

(24) SENSITIVE COVERED DATA.—

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

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

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

(iii) A financial account number, debit card number, credit card number, or information about income level or bank account balances.

(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, 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 is the sender or an intended recipient of the communication. Commu-

nications are not private for purposes of this paragraph 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 it 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 orientation or sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding disclosure of such information.

(x) Calendar information, address book information, phone or text logs, photos, audio recordings, or videos maintained for private use by an individual, regardless of whether such information is stored on the individual's device or in a separate location on an individual's device, regardless of whether such information is backed up in a separate location.

(xi) A photograph, film, video recording, or other similar medium that shows

the naked or undergarment-clad private area of an individual.

(xii) Information that reveals the video content or services requested or selected by an individual from a provider of broadcast television service, cable service, satellite service or streaming media service.

(xiii) Information about an individual when the covered entity knows that the individual is under the age of 17.

(xiv) Any other covered data collected, processed, or transferred for the purpose of identifying the above data types.

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

(25) SERVICE PROVIDER.—The term ''service provider'' means a person or entity that collects, processes or transfers covered data on behalf of, and

at the direction of, a covered entity and which receives covered data from or on behalf of a covered entity pursuant to a written contract, provided that the contract meets the requirements of section 302.

(26) 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 a covered entity for the purpose of allowing the service provider to perform a service or function on behalf of, and at the direction of, such covered entity.

(27) STATE.—The term ''State'' means any of the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, or the Trust Territory of the Pacific Islands.

(28) STATE PRIVACY AUTHORITY.—

(A) IN GENERAL.—The term ''State Privacy Authority'' means—

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

(ii) a State consumer protection agency with expertise in data protection.

(29) 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 material physical injury, economic injury, highly offensive intrusion into the reasonable privacy expectations of an individual under the circumstances, or discrimination on the basis of race, color, religion, national origin, sex, or disability.

(30) TARGETED ADVERTISING.—The term ''targeted advertising''—

(A) means displaying to an individual or device identified by a unique identifier an online advertisement or content 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;

(iii) contextual advertising, which is when an advertisement is displayed based on the content or location in which the advertisement appears and does not vary

based on who is viewing the advertisement; or

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

(31) THIRD PARTY.—The term ''third party''—

(A) means any person or entity that—

(i) collects, processes, or transfers third party 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 and share common branding, unless one of those is a large data holder or those entities are each related to a large data holder through common ownership or corporate control.

(32) 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 the 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 in so far 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, ''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 to which the covered data pertains.

(C) NON-APPLICATION TO SERVICE PROVIDERS.—An entity shall not be considered to

be a third-party collecting entity for purposes of this Act if the entity is acting as a service provider (as defined in this section).

(33) THIRD PARTY DATA.—The term ''third party data'' means covered data that has been transferred to a third party by a covered entity.

(34) TRANSFER.—The term ''transfer'' means – to disclose, release, share, disseminate, make available, or license in writing, electronically, or by any other means.

(35) UNIQUE IDENTIFIER.—The term ''unique identifier'' 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, an Internet Protocol address, cookies, beacons, pixel tags, mobile ad identifiers, or similar technology, customer number, unique pseudonym, or user alias, telephone numbers, or other forms of persistent or probabilistic identifiers that are linked or reasonably linkable to an individual or device.

(36) 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 tel-

evision, 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 shall 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;

(2) deliver a communication that is reasonably anticipated by the individual recipient within the context of the individual's interactions with the covered entity; or

(3) effect a purpose expressly permitted under subsection (b).

(b) PERMISSIBLE PURPOSES.—A covered entity or service provider may collect, process, or transfer covered data for any of the following purposes provided that the covered entity or service provider can demonstrate that collection, processing, or transfer complies with all other

applicable laws not preempted in section 404 and provisions of this Act and is limited to what is reasonably necessary and proportionate to such purpose:

(1) To initiate or complete a transaction or fulfill an order or service specifically requested by an individual, including any associated routine administrative activity such as billing, shipping, delivery, and accounting, including the collection, processing or transferring of the last four digits of a credit card number.

(2) With respect to covered data previously collected in accordance with this Act, notwithstanding this exception, to process such data as necessary to perform system maintenance or diagnostics, to maintain a product or service for which such data was collected, to conduct internal research or analytics, to improve a product or service for which such data was collected and to perform inventory management or reasonable network management, to protect against spam, or 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 prevent, detect, protect against, or respond to a security incident, or fulfill a product or service warranty. For purposes of this paragraph, security is defined as network security as well as intrusion, medical alerts, fire alarms, and access control security.

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

(6) To comply with a legal obligation imposed by Federal, Tribal, Local, or State law, or to establish, exercise, or defend legal claims.

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

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

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

(i) is in the public interest;

(ii) adheres to all relevant laws governing such research; and

(iii) adheres to the regulations for human subject research established under part 46 of title 45, Code of Federal Regulations (or a successor regulations).

(B) The Commission should set forth within 18 months of the enactment of this Act 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.

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

(11) With respect to covered data previously collected in accordance with this Act, notwithstanding this exception, to process such data as necessary to provide first party marketing or advertising of products or services provided by the covered entity.

(12) Otherwise complies with the requirements of this Act, including section 204(c), to provide a targeted advertisement.

(c) GUIDANCE.—The Commission shall issue guidance regarding what is reasonably necessary andproportionate 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 entities meeting the requirements of section 209, service provider, 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, service provider, or third party is prohibited from engaging in deceptive advertising or marketing with respect to a product or service provided to an individual.

SEC. 102. LOYALTY DUTIES.

(a) RESTRICTED DATA PRACTICES.—Notwithstanding section 101 and unless an exception applies, with respect to covered data, a covered entity shall not—

(1) collect, process, or transfer a social security number, except when necessary to facilitate extensions of credit, authentication, the payment and collection of taxes, the enforcement of a contract between parties, or the prevention, investigation, and prosecution of fraud or illegal activity;

(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 to effect a purpose enumerated in section 101(b)(1) through (10);

(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, or local law, or to establish, exercise, or defend legal claims; or

(C) the transfer is necessary to prevent an individual from imminent injury where the cov-

ered entity believes in good faith that the individual is at risk of death or serious physical injury;

(D) the transfer of biometric information is necessary to facilitate data security or authentication;

(E) the transfer of a password 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; or

(F) the transfer of genetic information 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)(9); or

(4) collect, process, or transfer an individual's aggregated internet search or browsing history, except with the affirmative express consent of the individual or pursuant to one of the permissible purposes enumerated in section 101(b)(1) through (10).

SEC. 103. PRIVACY BY DESIGN.

(a) POLICIES, PRACTICES, AND PROCEDURES.—A covered entity and a service provider shall establish, imple-

ment, and maintain reasonable policies, practices, and procedures regarding the collection, processing, and transfer of covered data to—

(1) consider 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 individuals under the age of 17, if applicable

(3) mitigate privacy risks, including substantial privacy risks, related to the products and services of the covered entity or the service provider, including their design, development, and implementation; 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.

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

(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, including whether the covered entity is a large data holder, nonprofit organization, covered entities meeting the requirements of section 209, third party, or third-party collecting entity;

(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 ap-

plicable to nonprofit organizations and covered entities meeting the requirements of section 209.

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

(a) CONDITIONAL SERVICE OR PRICING PROHIBITED.—A covered entity shall not deny or condition or effectively condition the provision of a service or product to an individual based on the individual's agreement to waive (or refusal to waive) any requirements under this Act or any regulations promulgated under this Act or terminate a service or otherwise refuse to provide a service or product to an individual as a consequence of the individual's refusal to provide such a waiver.

(b) RULES OF CONSTRUCTION.—Nothing in subsection (a) shall 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 loyalty program that provides discounted or free products or services, or other consideration, in ex-

change for an individual's continued business with the covered entity, provided that such program otherwise complies with the requirements of this Act and any regulations promulgated under this Act;

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

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

(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 in section 203(a)(3).

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 materials disclosed pursuant to subsection (a) in the ten languages with the most users in the United States, according to the most recent U.S. Census. The Commission shall ensure the website is readily accessible to and usable by individuals with disabilities.

SEC. 202. TRANSPARENCY.

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

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

(1) The identity and the contact information of—

(A) the covered entity or service provider (including the covered entity's or service provider's points of contact, generic electronic mail addresses, and phone numbers of the covered entity, as applicable for privacy and data security inquiries); and

(B) any other entity within the same corporate structure as, and under common branding with, 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 en-

tities, except for transfers to governmental entities pursuant to a court order or law that prohibits the covered entity from disclosing such 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 time frame, the criteria used to determine the length of time the covered entity 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 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 readily 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 previously collected covered data and, except as provided in section 101(b), provide a reasonable opportunity for each individual to withdraw consent to any further materially different collection, processing or transferring of covered data under the changed policy.

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

(3) CLARIFICATION.—Nothing in this section shall 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 and publish them on its website. It shall make publicly available, in a clear, conspicuous, and readily accessible manner, a log describing the data and nature of each material change over the past 10 years. The descriptions shall be sufficient for a reasonable individual to understand the material effect of each material change.

(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 must provide a short-form notice of its covered data practices in a manner that is—

(A) concise, clear, and conspicuous;

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

(C) inclusive of an overview of individual rights and disclosures to reasonably draw attention to data practices that may reasonably be unexpected 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 which shall not exceed the content requirements in subsection (b) and shall include templates and/or models of short-form notices.

SEC. 203. INDIVIDUAL DATA OWNERSHIP AND CONTROL.

(a) ACCESS TO, AND CORRECTION, DELETION, AND PORTABILITY OF, COVERED DATA.—Subject to 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) the covered data, except covered data in back-up or archival systems, of the individual in a human-readable format that a reasonable individual can understand and download from the Internet, 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 name of any third party 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 verifiably material inaccuracy or materially incomplete information with respect to the covered data of the individual that is processed by the covered entity and instruct the covered entity to notify any third party, or service provider to which the covered entity transferred such covered data of the corrected information;

(3) delete covered data of the individual that is processed by the covered entity and instruct the covered entity to notify any third party, or service provider to which the covered entity transferred such covered data of the individual's deletion request; and

(4) to the extent technically feasible, export covered data to the individual or directly to another entity, except for derived data, of the individual that is processed by the covered entity 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 shall not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of any individual rights under this section through—

(1) through 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 rights.

(c) TIMING.—

(1) Subject to subsections (d) and (e)(1) each request shall be completed by any—

(A) large data holder within 45 days of verification of such request from an individual;

(B) covered entity that is not considered a large data holder or a covered entity described in section 209 within 60 days of verification of such request from an individual; or

(C) covered entity as described in section 209 within 90 days of verification of such request from an individual.

(2) 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 shall 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; or

(D) reasonably believes that the exercise of the right would require the covered entity to en-

gage in an unfair or deceptive practice under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

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

(3) PERMISSIVE EXCEPTIONS.—

(A) IN GENERAL.—A covered entity may decline 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 impossible or demonstrably impracticable 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) result in the release of trade secrets, or other privileged, or confidential business information;

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

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

(vii) violate Federal or State law or the rights and freedoms of another indi-

vidual, including under the Constitution of the United States;

(viii) 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 who has submitted a deletion request and requests that the covered entity no longer collect, process, or transfer such data;

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

(x) 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; or

(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.

(B) PARTIAL COMPLIANCE.—In a circumstance that would allow a denial pursuant to paragraph (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 this paragraph, the receipt of a large number of verified requests, on its own, shall not be considered to render compliance with a request demonstrably impossible.

(D) FURTHER EXCEPTIONS.—The Commission may, by regulation as described in subsection (f), establish additional permissive ex-

ceptions 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 creating 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) REGULATIONS.—Within two years of the date of enactment of this Act, the Commission may promulgate regulations, pursuant to section 553 of title 5, United States Code (5 U.S.C. 553), 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 entities meeting the requirements of section 209, service provider, 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.

(g) ACCESSIBILITY.—A covered entity shall facilitate the ability for individuals to make requests under this section in any of the ten languages with the most users in the United States, according to the most recent U.S. Census, if the covered entity provides service in such language. The mechanisms by which a covered entity enables individuals to make requests under this section shall be readily accessible and usable by 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) shall not transfer 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 transfer through an opt-out mechanism, as described in section 210, if applicable.

(2) EXCEPTION.—An individual may not opt out of the collection, processing, and transfer of covered data made pursuant to the exceptions in section 101(b)(1) through (11) of this Act.

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

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

(2) abide by such opt-out designations by an individual; and

(3) allow an individual to prohibit such targeted advertising through an opt-out mechanism, as described in section 210, if applicable.

(d) INDIVIDUAL AUTONOMY.—A covered entity shall not condition, effectively condition, attempt to condition,

or attempt to effectively condition the exercise of any individual rights under this section through—

(1) through 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 rights.

SEC. 205. DATA PROTECTIONS FOR CHILDREN AND MINORS.

(a) PROHIBITION ON TARGETED ADVERTISING TO CHILDREN AND MINORS.—A covered entity shall not engage in targeted advertising to any individual under the age of 17 if the covered entity knows that the individual is under the age of 17.

(b) DATA TRANSFER REQUIREMENTS RELATED TO MINORS.—A covered entity shall not transfer the covered data of an individual to a third party without affirmative express consent from the individual or the individual's parent or guardian if the covered entity knows that the individual under the age of 17.

(c) KNOWLEDGE .—The knowledge requirement in paragraphs (a) and (b), shall not be construed to require

the affirmative collection or processing of any data with respect to the age of an individual or a proxy thereof, or to require that a covered entity implement an age gating regime. Rather, the determination of whether an individual is under 17 shall be based on the covered data collected directly from an individual or a proxy thereof that the covered entity would otherwise collect in the normal course of business.

(d) YOUTH PRIVACY AND MARKETING DIVISION.—

(1) ESTABLISHMENT.—There is established within the Commission a division to be known as the ''Youth Privacy and Marketing Division'' (in this 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 1 year 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, assisting 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.

(e) 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 1307 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 and conspicuous 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; and

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

(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 data the third-party collecting entity processes and transfers.

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

(iv) 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 al-

lows members of the public to identify individual third-party collecting entities.

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

(C) A ''Do Not Collect'' registry link and mechanism by which an individual may, after the Commission has verified the identity of the individual or individual's parent or guardian, which may include tokenization, easily submit a request to all registered third-party collecting entities that are not consumer reporting agencies, and to the extent they are not acting as consumer reporting agencies, as defined in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) to—

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

(ii) ensure that any third-party collecting entity no longer collects covered data related to such individual without the affirmative express consent of such indi-

vidual, except insofar as such covered entity is acting as a service provider. 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.

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

(1) a civil penalty of $50 for each day it fails to register or provide notice as required under this subsection, not to exceed a total of $10,000 for any year; and

(2) an amount equal to the registration fees due under paragraph (2) of subsection (b) for each year that it failed to register as required under paragraph (1) of such subsection.

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 Federal 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 Federal agencies.

(c) ALGORITHM IMPACT AND EVALUATION.—

(1) 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 an algorithm that may cause potential harm to an individual, and uses such al-

gorithm solely or in part, to collect, process or transfer covered data must 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 algorithm.

(ii) A statement of the purpose, proposed uses, and foreseeable capabilities outside of the articulated proposed use of the algorithm.

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

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

(v) An assessment of the necessity and proportionality of the algorithm in relation to its stated purpose, including reasons for the superiority of the algorithm

over nonautomated decision making methods; and

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

(I) any individual under the age of 17;

(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; or

(IV) disparate impact on the basis of individuals' race, color, religion, national origin, sex, or disability 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 an algorithm, solely or in part, to collect, process or transfer covered data or publicly available information shall prior to deploying the algorithm in interstate commerce evaluate the design, structure, and inputs of the algorithm, including any training data used to develop the algorithm, to reduce the risk of the potential harms identified under paragraph (1)(B).

(3) OTHER CONSIDERATIONS.—

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

(B) EXTERNAL, INDEPENDENT AUDITOR OR RESEARCHER.—To the extent possible, a covered entity and a service provider shall utilize an external, independent auditor or researcher to conduct an impact assessment

under paragraph (1) or an evaluation under paragraph (2).

(C) 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 and evaluation conducted under paragraphs (1) and (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 must make all submissions under this section to the Commission in unredacted form, but a covered entity and a service provider may redact and segregate any trade secrets (as defined in section 1839 of title 18, United States

Code) from public disclosure under this subparagraph.

(D) 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, including the study and report provisions in paragraph 6 of this section. This provision shall not preclude the Commission from providing this information to Congress in response to a subpoena or official Congressional request.

(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)(C)(i)(I); and

(B) may exclude from this subsection any algorithm that presents low or minimal risk for potential for harms to individuals (as identified under paragraph (1)(B)).

(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 paragraph. Such study shall include an examination of—

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

(ii) methods to reduce the risk of harm to individuals that may be related to the use of 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 subsection (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 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 required under subsection (a) shall include, 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 respond to unsolicited reports of vulnerabilities by any entity or individual.

(2) PREVENTIVE AND CORRECTIVE ACTION.—Taking preventive and corrective action designed to mitigate any 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, which may include implementing administrative, technical, or physical safeguards or changes to data security practices or the architecture, installation, or implementation of network or operating software, among other actions.

(3) EVALUATION OF PREVENTIVE AND CORRECTIVE ACTION.—Evaluating and making reasonable adjustments to the safeguards 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 that 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.

(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 or 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.

(d) APPLICABILITY OF OTHER INFORMATION SECURITY LAWS.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) or the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), and is in compliance with the information security requirements of such Act as determined by the enforcement authority in such Act, shall be deemed to be in compliance with the requirements of this section with respect to any data covered by such information security requirements.

SEC. 209. SMALL BUSINESS PROTECTIONS.

(a) IN GENERAL.—

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

(A) be exempt from compliance with sections 203(a)(4), 208(b)(1)–(3), (5)-–(7), 301(c); and

(B) 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.

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

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

(B) The covered entity or service provider, on average, did not annually collect or process the covered data of more than 200,000 individuals during the period beyond the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product, so long as all covered data for such purpose is deleted or de-identified within 90 days.

(C) The covered entity or service provider did not derive more than 50 percent of its rev-

enue from transferring covered data during any year (or part of a year if the covered entity has been in existence for less than 1 year) that occurs during the period.

(3) DEFINITION.—For purposes of this section, the term ''revenue'' as it relates to any covered entity that is not organized to carry on business for its own profit or that of their members, means the gross receipts the covered entity 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.

(4) JOURNALISM.—Nothing in this Act shall be construed to limit or diminish First Amendment freedoms to gather and publish information guaranteed under the Constitution.

SEC. 210. UNIFIED OPT-OUT MECHANISMS.

For the rights established under sections 204(b) and (c), and section 206(c)(3)(D) not later than 18 months after the date of enactment of this Act, the Commission shall establish one or more acceptable privacy protective, centralized mechanisms, including global privacy signals such as browser or device privacy settings, for individuals

to exercise all such rights through a single interface for a covered entity to utilize to allow an individual to make such opt out designations with respect to covered data related to such individual.

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) reporting structures to ensure that such certifying officers are involved in, and are responsible for, decisions that impact the entity's compliance with this Act.

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

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

(1) IN GENERAL.—A covered entity and a service provider 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 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) of this subsection to report directly to the highest official at the large data holder as a privacy protection officer who shall, in addition to the re-

quirements 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 work to ensure the company is in compliance with all applicable laws and ensure such audits are accessible to the Commission upon such request;

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

(D) maintain updated, accurate, clear, and understandable records of all 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 that a covered entity or service provider first meets the definition of large data holder, whichever is earlier, and biennially thereafter, each large data holder shall conduct a privacy impact assessment that weighs the benefits of the large data holder's covered data collecting, processing, and transfer practices against the potential 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 large data holder;

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

(iii) the potential 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.

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

SEC. 302. SERVICE PROVIDERS AND THIRD PARTIES.

(a) SERVICE PROVIDERS.—A service provider—

(1) shall only collect, process, and transfer service provider data to the extent strictly necessary and proportionate to provide a service requested by the covered entity. This paragraph shall not require a service provider to collect or process covered data if the service provider would not otherwise do so;

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

(3) shall assist a covered entity in fulfilling the covered entity's obligation to respond to individual rights requests pursuant to section 203, by appropriate technical and organizational measures, taking into account the nature of the processing and the information reasonably available to the service provider;

(4) may engage another service provider for purposes of processing service provider data on behalf of a covered entity only after providing the covered entity that is directing the services or functions of the service provider with respect to such service provider data 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;

(5) shall upon the reasonable request of the covered entity, make available to the covered entity information necessary to demonstrate the service provider's compliance with the obligations in this Act, which may include making available a report of an independent assessment arranged by the service provider on terms agreed to by the parties and making the report required under section 207(c)(2) as applicable;

(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 not transfer service provider data to any person with the exception of another service provider without the affirmative express consent, obtained by the covered entity with the direct relationship to the individual that is directing the services or functions of the service provider with respect to the service provider data, of the individual to whom the service provider data is linked or reasonably linkable;

(8) shall develop, implement, and maintain reasonable administrative, technical, and physical safeguards that are designed to protect the security and confidentiality of covered data it processes consistent with section 208; and

(9) shall be exempt from the requirements of section 202(d) with respect to service provider data but shall provide direct notification regarding material changes to its privacy policy to each covered entity with which it provides services or functions as a service provider, in each language that the privacy

policy is made available. Compliance with this provision does not alleviate any obligations the service provider has to the covered entity to which it provides services or functions as a service provider.

(b) CONTRACTS BETWEEN COVERED ENTITIES AND SERVICE PROVIDERS.—A person or entity may 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 permitted in section 302(a)(4), provided that the contract—

(1) governs the service provider's data processing procedures with respect to processing or transfer performed on behalf of the covered entity or service provider;

(2) clearly sets forth—

(A) instructions for processing data;

(B) the nature and purpose of processing;

(C) the type of data subject to processing;

(D) the duration of processing; and

(E) the rights and obligations of both parties; and

(3) does not relieve a covered entity or a service provider of an obligation under this Act; and

(4) prohibits—

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

(B) combining service provider data with covered data which the service provider receives from or on behalf of another person or persons or collects from its own interaction with an individual. The contract may, subject to agreement with the service provider, permit a covered entity to monitor the service provider's compliance with the contract through measures including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(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 data is a fact-based determination that depends upon the context in which such data is processed.

(2) A covered entity or service provider that transfers covered data to a service provider, in compliance with the requirements of this Act, is not lia-

ble for a violation of this Act by the service provider to whom such covered data was transferred, this Act provided that, at the time of transferring such covered data, the covered entity or service provider did not know or have reason to know that the service provider would likely commit a violation of this Act.

(3) 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 it receives such covered data.

(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 and, in the case of non-sensitive data, the processing purpose for which the covered entity made a disclosure pursuant to section 204(b)(4);

(2) for purposes of paragraph (1), may reasonably rely on representations made by the covered entity that transferred the third party data , provided that the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible; and

(3) shall be exempt from the requirements of section 204 with respect to third party data, but shall otherwise have the same responsibilities and obligations as a covered entity with respect to such data under all other provisions of this Act.

(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 small- and medium-sized covered entities.

SEC. 303. TECHNICAL COMPLIANCE PROGRAMS.

(a) IN GENERAL.—Not later than 1 year after the date of the 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 specific to any technology, product, service, or

method 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 guidelines for compliance with this Act;

(2) meet or exceed the requirements of this Act; and

(3) be made publicly available to any individual whose covered data is collected, processed, or transferred using such technology, product, service, or method.

(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, 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 180 days after the filing of the request, and shall set forth publicly in writing its conclusions 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 180 day 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 enforce-

ment action described in Sec. 403 is commenced, 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 deliberations or activities or impose any pleading requirement on the Commission should it bring 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 proposal 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 of 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 must 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 180 days 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 its determination to withdraw approval of such guidelines and the basis for doing so. Upon 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 within 180 days and submit the proposed cure or cures 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 it 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, except that the definition developed pursuant to this section shall not supersede any other provision of

law or be construed to limit the authority of any executive agency related to digital content forgeries.

(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) NEW BUREAU.—

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

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

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

(b) OFFICE OF BUSINESS MENTORSHIP.—The Director of the Bureau established under subsection (a) shall establish within the Bureau an Office of Business Mentorship to provide guidance and education to covered entities regarding compliance with this Act. Covered entities may request advice from the Commission or this office

with respect to a course of action which the covered entity proposes to pursue and which 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 under this Act 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 NONPROFITS.—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 subsections (1), (2), (3), and (5) of this subsection, 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) DATA PRIVACY AND SECURITY VICTIMS RELIEF FUND.—

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

(B) DEPOSITS.—

(i) DEPOSITS.—The amount of any civil penalty obtained against any covered entity or service provider or any other relief ordered to provide redress, payments or compensation, or other monetary relief to individuals that cannot be located or the payment of which would otherwise not be practicable in any judicial or administrative action to enforce this Act or a regulation promulgated under this Act shall be deposited into the Victims Relief Fund.

(C) USE OF FUND AMOUNTS.—

(i) AVAILABILITY TO THE COMMISSION.—Notwithstanding section 3302 of title 31, United States Code, amounts in the Victims Relief Fund shall be available

to the Commission, without fiscal year limitation, to provide redress, payments or compensation, or other monetary relief to individuals affected by an act or practice for which relief has been obtained under this Act.

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

(I) 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 STATE ATTORNEYS GENERAL.

(a) CIVIL ACTION.—In any case in which the attorney general of a State or State Privacy Authority has reason to believe that an interest of the residents of that state has been, may be, or is adversely affected by the engagement of any a covered entity or service provider in an act

or practice that has violated this Act or a regulation promulgated under this Act, the attorney general of the State, 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 that act or practice;

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

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

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

(b) RIGHTS OF THE COMMISSION.—

(1) IN GENERAL.—Except where not feasible, the attorney general of a State or State Privacy Authority shall notify the Commission in writing prior to initiating a civil action under subsection (a). Such notice shall include a copy of the complaint to be filed to initiate such action. Upon receiving such notice, the Commission may intervene in such action as of right pursuant to the Federal Rules of Civil Procedure.

(2) NOTIFICATION TIMELINE.—Where it is not feasible for the attorney general of a State or State Privacy Authority to provide the notification required by paragraph (1) before initiating a civil action under subsection (a), the attorney general of a State 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 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 violation of this Act or a regulation promulgated under this Act that is alleged in such complaint, if the Commission's complaint alleges such violations affected the residents of the relevant state or individuals nationwide. In a case brought by the Commission that affects the interests of a State, an attorney general of such state or State Privacy Authority may intervene as of right pursuant to the Federal Rules of Civil Procedure.

(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to prevent the attorney general of

a State or State Privacy Authority 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), no provision of this section shall be construed as altering, limiting, or affecting the authority of a State attorney general or State Privacy Authority to—

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

(2) exercise the powers conferred on the attorney general 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 INDIVIDUALS.

(a) ENFORCEMENT BY INDIVIDUALS.—

(1) IN GENERAL.—Beginning 4 years after the date on which this Act takes effect, any individual who suffers an injury that could be addressed by the relief permitted in paragraph (2) for a violation of

this Act or a regulation promulgated under this Act by a covered entity 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 the plaintiff prevails, the court may award the plaintiff—

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

(B) injunctive relief; and

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

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

(A) IN GENERAL.—Prior to an individual bringing a civil action under paragraph (1), such individual must first notify the Commission and the attorney general of the State of the individuals residence in writing outlining their desire to commence a civil action. Upon receiving such notice, the Commission and State attorney general shall make a determination, not later than 60 days after receiving such notice, as to whether they will independently

seek to intervene in such action, and upon intervening—

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

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

(B) BAD FAITH.—Any written communication requesting a monetary payment that is sent to a covered entity 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:

(i) 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).

(ii) After the Commission or attorney general of a State made the determination to independently seek civil actions against such entity as outlined in subparagraph (A).

(4) FTC STUDY.—Beginning on the date that is 5 years after the date of enactment of this Act, the Commission's Bureau of Economics shall conduct an annual study to determine the economic im-

pacts in the United States of demand letters and the scope of the rights of an individual to bring forth civil actions against covered entities. Such study shall include, but not be limited to include the following:

(A) The impact on increasing 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 startup companies, including tech startup companies.

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

(5) REPORT TO CONGRESS.—Not later than 1 year after the first day on which individuals 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) PRE-DISPUTE ARBITRATION AGREEMENTS AND PRE-DISPUTE JOINT ACTION WAIVERS RELATED TO INDIVIDUALS UNDER THE AGE OF 18.—

(1) ARBITRATION.—Except as provided in section 303(d), and notwithstanding any other provision of law, no agreement for pre-dispute arbitration with respect to an individual under the age of 18 may limit any of the rights provided in this Act.

(2) JOINT ACTION WAIVERS.—Notwithstanding any other provision of law, no agreement for pre-dispute joint action waiver with respect to an individual under the age of 18 may limit any of the rights provided in 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 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), any action under this section may be brought by an individual if, prior to initiating such action against a covered entity for injunctive relief or against a covered entity that meets the requirements of section 210(c) for any form of relief the individual provides to the covered entity 45 days' written notice identifying the specific provisions of this Act the individual alleges have been or are being violated.

(2) EFFECT OF CURE.—In the event a cure is possible, if within the 45 days the covered entity cures the noticed violation and provides the individual an express written statement that the violation has been cured and that no further violations shall occur, an action for injunctive relief may be reasonably dismissed.

(d) DEMAND LETTER.—If an individual or a class of individuals sends correspondence to a covered entity alleging a violation of the provisions of this Act and request-

ing a monetary payment, such correspondence shall include the following language: ''Please visit the website of the Federal Trade Commission to understand your rights pursuant to this letter'' followed by a hyperlink to the webpage of the Commission required under section 201. If such correspondence does not include such language and hyperlink, the individual or joint class of individuals shall forfeit their rights under this section.

(e) APPLICABILITY.—This section shall only apply to any claim alleging a violation of section 102, 104, 202, 203, 204, 205(a), 205(b), 206(c)(3)(D), 207(a), 208(a), or 302 for which relief described in subsection (a)(2) may be granted.

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 shall 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, regarding information security breaches; or

(C) any other provision of Federal law unless specifically authorized by this Act.

(2) 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), 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 title, except for section 208, 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.

(3) 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 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, 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) shall not be construed to preempt, displace, or supplant the following State laws, rules, regulations, or requirements:

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

(B) Civil rights laws.

(C) Laws 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 governing fraud, theft, including identity theft, unauthorized access to information or electronic devices, or unauthorized use of information, malicious behavior, or similar provisions, or laws of criminal procedure.

(G) Criminal or civil laws regarding cyberstalking, cyberbullying, nonconsensual pornography, or sexual harassment.

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

(I) Laws that address public records, criminal justice information systems, arrest records, mug shots, conviction records, or nonconviction records.

(J) Laws that address banking records, financial records, tax records, Social Security numbers, credit cards, credit reporting and investigations, credit repair, credit clinics, or check-cashing services.

(K) Laws that solely address facial recognition or facial recognition technologies, electronic surveillance, wiretapping, or telephone monitoring.

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

(M) Laws to address unsolicited email messages, telephone solicitation, or caller ID.

(N) Laws that address health information, medical information, medical records, HIV status, or HIV testing.

(O) Laws that address the confidentiality of library records.

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

(3) NONAPPLICATION OF FCC PRIVACY LAWS AND REGULATIONS TO COVERED ENTITIES.—Notwithstanding any other provision of law, Sections 222, 338(i), and 631 of the Communications Act of 1934, as amended, (47 U.S.C. §§ 222, 338(i), and 551) and any regulation promulgated by the Federal Communications Commission under such sections, shall not apply to any covered entity with respect to the collecting, processing, or transferring of covered data under this Act.

(c) PRESERVATION OF COMMON LAW OR STATUTORY CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this Act, nor any amendment, standard, rule, requirement, assessment, law or regulation promulgated under this Act, shall be construed to preempt, displace, or supplant any Federal or State common law 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, except that the fact of a violation of this Act shall not be pleaded as an element of any such cause of action.

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 shall be construed to relieve or change any obligations that a covered entity or another 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 enactment of this Act, the Commission shall amend its rules issued pursuant to 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 those already enacted under the Children's Online Privacy Protection Act of 1998 that may already apply to some of such covered entities.

SEC. 407. AUTHORIZATION OF APPROPRIATIONS.

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

SEC. 408. EFFECTIVE DATE.

Except as otherwise provided, this Act shall take effect on the date that is 180 days after the date of enactment of this Act.