II

117TH CONGRESS
1ST SESSION

S. 2499

To establish data privacy and data security protections for consumers in the United States.

IN THE SENATE OF THE UNITED STATES

JULY 28, 2021

Mr. WICKER (for himself and Mrs. BLACKBURN) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To establish data privacy and data security protections for consumers in the United States.

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 ''Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act'' or the ''SAFE DATA Act''.

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

SEC. 2. DEFINITIONS.

In this Act:

(1) AFFIRMATIVE EXPRESS CONSENT.—The term ''affirmative express consent'' means, upon being presented with a clear and conspicuous description of an act or practice for which consent is sought, an affirmative act by the individual clearly communicating the individual's authorization for the act or practice.

(2) ALGORITHM.—The term ''algorithm'' means a computational process derived from machine learn-

ing, statistics, or other data processing or artificial intelligence techniques, that processes covered data for the purpose of making a decision or facilitating human decision-making.

(3) COLLECTION.—The term ''collection'' means buying, renting, gathering, obtaining, receiving, or accessing any covered data of an individual by any means.

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

(5) COMMON BRANDING.—The term ''common branding'' means a shared name, servicemark, or trademark.

(6) COVERED DATA.—

(A) IN GENERAL.—The term ''covered data'' means information that identifies or is linked or reasonably linkable to an individual or a device that is linked or reasonably linkable to an individual.

(B) LINKED OR REASONABLY LINKABLE.—For purposes of subparagraph (A), information held by a covered entity is linked or reasonably linkable to an individual or a device if, as a practical matter, it can be used on its own or in combination with other information held by,

or readily accessible to, the covered entity to identify such individual or such device.

(C) EXCLUSIONS.—Such term does not include—

(i) aggregated data;

(ii) de-identified data;

(iii) employee data; or

(iv) publicly available information.

(D) AGGREGATED DATA.—For purposes of subparagraph (C), the term ''aggregated data'' means information that relates to a group or category of individuals or devices that does not identify and is not linked or reasonably linkable to any individual or device.

(E) DE-IDENTIFIED DATA.—For purposes of subparagraph (C), the term ''de-identified data'' means information held by a covered entity that—

(i) does not identify, and is not linked or reasonably linkable to, an individual or device;

(ii) does not contain any persistent identifier or other information that could readily be used to reidentify the individual

to whom, or the device to which, the identifier or information pertains;

(iii) is subject to a public commitment by the covered entity—

(I) to refrain from attempting to use such information to identify any individual or device; and

(II) to adopt technical and organizational measures to ensure that such information is not linked to any individual or device; and

(iv) is not disclosed by the covered entity to any other party unless the disclosure is subject to a contractually or other legally binding requirement that—

(I) the recipient of the information shall not use the information to identify any individual or device; and

(II) all onward disclosures of the information shall be subject to the requirement described in subclause (I).

(F) EMPLOYEE DATA.—For purposes of subparagraph (C), the term ''employee data'' means—

(i) information relating to an individual collected by a covered entity in the course of the individual acting as a job applicant to, or employee (regardless of whether such employee is paid or unpaid, or employed on a temporary basis), owner, director, officer, staff member, trainee, vendor, visitor, volunteer, intern, or contractor of, the entity, provided that such information is collected, processed, or transferred by the covered entity solely for purposes related to the individual's status as a current or former job applicant to, or an employee, owner, director, officer, staff member, trainee, vendor, visitor, volunteer, intern, or contractor of, that covered entity;

(ii) business contact information of an individual, including the individual's name, position or title, business telephone number, business address, business email address, qualifications, and other similar information, that is provided to a covered entity by an individual who is acting in a professional capacity, provided that such

information is collected, processed, or transferred solely for purposes related to such individual's professional activities;

(iii) emergency contact information collected by a covered entity that relates to an individual who is acting in a role described in clause (i) with respect to the covered entity, provided that such information is collected, processed, or transferred solely for the purpose of having an emergency contact on file for the individual; or

(iv) information relating to an individual (or a relative or beneficiary of such individual) that is necessary for the covered entity to collect, process, or transfer for the purpose of administering benefits to which such individual (or relative or beneficiary of such individual) is entitled on the basis of the individual acting in a role described in clause (i) with respect to the entity, provided that such information is collected, processed, or transferred solely for the purpose of administering such benefits.

(G) PUBLICLY AVAILABLE INFORMATION.—

(i) IN GENERAL.—For the purposes of subparagraph (C), the term ''publicly available information'' means any information that a covered entity has a reasonable basis to believe—

(I) has been lawfully made available to the general public from Federal, State, or local government records;

(II) is widely available to the general public, including information from—

(aa) a telephone book or online directory;

(bb) television, internet, or radio content or programming; or

(cc) the news media or a website that is lawfully available to the general public on an unrestricted basis (for purposes of this subclause a website is not restricted solely because there is a fee or log-in requirement associ-

ated with accessing the website); or

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

(ii) EXCLUSIONS.—Such term does not include an obscene visual depiction (as defined for purposes of section 1460 of title 18, United States Code).

(7) COVERED ENTITY.—The term ''covered entity'' means any person that—

(A) is subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.) or is—

(i) a common carrier described in section 5(a)(2) of such Act (15 U.S.C. 45(a)(2)); or

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

(B) collects, processes, or transfers covered data; and

(C) determines the purposes and means of such collection, processing, or transfer.

(8) DATA BROKER.—

(A) IN GENERAL.—The term ''data broker'' means a covered entity whose principal source of revenue is derived from processing or transferring the covered data of individuals with whom the entity does not have a direct relationship on behalf of third parties for such third parties' use.

(B) EXCLUSION.—Such term does not include a service provider.

(9) DELETE.—The term ''delete'' means to remove or destroy information such that it is not maintained in human or machine readable form and cannot be retrieved or utilized in such form in the normal course of business.

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

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

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

(A) processed or transferred the covered data of more than 8,000,000 individuals; or

(B) processed or transferred the sensitive covered data of more than 300,000 individuals or devices that are linked or reasonably linkable to an individual (excluding any instance where the covered entity processes the 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).

(13) 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), that such act, practice, or representation is likely to affect an individual's decision or conduct regarding a product or service.

(14) PROCESS.—The term ''process'' means any operation or set of operations performed on covered data including analysis, organization, structuring, retaining, using, or otherwise handling covered data.

(15) PROCESSING PURPOSE.—The term ''processing purpose'' means a reason for which a covered entity processes covered data.

(16) RESEARCH.—The term ''research'' means the scientific analysis of information, including cov-

ered data, by a covered entity or those with whom the covered entity is cooperating or others acting at the direction or on behalf of the covered entity, that is conducted for the primary purpose of advancing scientific knowledge and may be for the commercial benefit of the covered entity.

(17) SENSITIVE COVERED DATA.—

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

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

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

(iii) A financial account number, debit card number, credit card number, or any required security or access code, password, or credentials allowing access to any such account.

(iv) Covered data that is biometric information.

(v) Precise geolocation information.

(vi) A persistent identifier.

(vii) The contents of an individual's private communications, such as emails, texts, direct messages, or mail, or the identity of the parties subject to such communications, unless the covered entity is the intended recipient of the communication.

(viii) Account log-in credentials such as a user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(ix) Covered data revealing an individual's racial or ethnic origin, or religion in a manner inconsistent with the individual's reasonable expectation regarding the processing or transfer of such information.

(x) Covered data revealing the sexual orientation or sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regard-

ing the processing or transfer of such information.

(xi) Covered data about the online activities of an individual that addresses or reveals a category of covered data described in another clause of this subparagraph.

(xii) Covered data that is calendar information, address book information, phone or text logs, photos, or videos maintained for private use on an individual's device.

(xiii) Any covered data collected or processed by a covered entity for the purpose of identifying covered data described in another clause of this subparagraph.

(xiv) Any other category of covered data designated by the Commission pursuant to a rulemaking under section 553 of title 5, United States Code.

(B) BIOMETRIC INFORMATION.—For purposes of subparagraph (A), the term ''biometric information''—

(i) means the physiological or biological characteristics of an individual, includ-

ing deoxyribonucleic acid, that are used, singly or in combination with each other or with other identifying data, to establish the identity of an individual; and

(ii) includes—

(I) imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted; and

(II) keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(C) PERSISTENT IDENTIFIER.—For purposes of subparagraph (A), the term ''persistent identifier'' means a technologically derived identifier that identifies an individual, or is linked or reasonably linkable to an individual over time and across services and platforms, which may include a customer number held in a cookie, a static Internet Protocol address, a processor or device serial number, or another unique device identifier.

(D) PRECISE GEOLOCATION INFORMATION.—For purposes of subparagraph (A), the term ''precise geolocation information'' means technologically derived information capable of determining the past or present actual physical location of an individual or an individual's device at a specific point in time to within 1,750 feet.

(18) SERVICE PROVIDER.—The term ''service provider'' means, with respect to a set of covered data, a covered entity that processes or transfers such covered data for the purpose of performing 1 or more services or functions on behalf of, and at the direction of, a covered entity that—

(A) is not related to the covered entity providing the service or function by common ownership or corporate control; and

(B) does not share common branding with the covered entity providing the service or function.

(19) SERVICE PROVIDER DATA.—The term ''service provider data'' means covered data that is collected by the service provider on behalf of a covered entity or transferred to the service provider by a covered entity for the purpose of allowing the serv-

ice provider to perform a service or function on behalf of, and at the direction of, such covered entity.

(20) THIRD PARTY.—The term ''third party'' means, with respect to a set of covered data, a covered entity—

(A) that is not a service provider with respect to such covered data; and

(B) that received such covered data from another covered entity—

(i) that is not related to the covered entity by common ownership or corporate control; and

(ii) that does not share common branding with the covered entity.

(21) THIRD PARTY DATA.—The term ''third party data'' means, with respect to a third party, covered data that has been transferred to the third party by a covered entity.

(22) TRANSFER.—The term ''transfer'' means to disclose, release, share, disseminate, make available, or license in writing, electronically, or by any other means for consideration of any kind or for a commercial purpose.

SEC. 3. EFFECTIVE DATE.

Except as otherwise provided in this Act, this Act shall take effect 18 months after the date of enactment of this Act.

TITLE I—INDIVIDUAL CONSUMER DATA RIGHTS

SEC. 101. CONSUMER LOYALTY.

(a) PROHIBITION ON THE DENIAL OF PRODUCTS OR SERVICES.—

(1) IN GENERAL.—Subject to paragraph (2), a covered entity shall not deny products or services to an individual because the individual exercises a right established under subparagraph (A), (B), or (D) of section 103(a)(1).

(2) RULES OF APPLICATION.—A covered entity—

(A) shall not be in violation of paragraph (1) with respect to a product or service and an individual if the exercise of a right described in such paragraph by the individual precludes the covered entity from providing such product or service to such individual; and

(B) may offer different types of pricing and functionalities with respect to a product or service based on an individual's exercise of a right described in such paragraph.

(b) NO WAIVER OF INDIVIDUAL CONTROLS.—The rights and obligations created under section 103 may not be waived in an agreement between a covered entity and an individual.

SEC. 102. TRANSPARENCY.

(a) IN GENERAL.—A covered entity that processes covered data shall, with respect to such data, publish a privacy policy that is—

(1) disclosed, in a clear and conspicuous manner, to an individual prior to or at the point of the collection of covered data from the individual; and

(2) made available, in a clear and conspicuous manner, to the public.

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

(1) The identity and the contact information of the covered entity (including the covered entity's points of contact for privacy and data security inquiries) and the identity of any affiliate to which covered data may be transferred by the covered entity.

(2) The categories of covered data the covered entity collects.

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

(4) Whether the covered entity transfers covered data, the categories of recipients to whom the covered entity transfers covered data, and the purposes of the transfers.

(5) A general description of the covered entity's data retention practices for covered data and the purposes for such retention.

(6) How individuals can exercise their rights under section 103.

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

(8) The effective date of the privacy policy.

(c) LANGUAGES.—A privacy policy required under subsection (a) shall be made available in all of the languages in which the covered entity provides a product or service that is subject to the policy, or carries out activities related to such product or service.

(d) MATERIAL CHANGES.—If a covered entity makes a material change to its privacy policy, it shall notify the individuals affected before further processing or transferring of previously collected covered data and, except as provided in section 108, provide an opportunity to withdraw consent to further processing or transferring of the

covered data under the changed policy. The covered entity shall provide direct notification, where possible, regarding a material change to the privacy policy to affected individuals, taking into account available technology and the nature of the relationship.

(e) APPLICATION TO INDIRECT TRANSFERS.—Where the ownership of an individual's device is transferred directly from one individual to another individual, a covered entity may satisfy its obligation to disclose a privacy policy prior to or at the point of collection of covered data by making the privacy policy available under subsection (a)(2).

SEC. 103. INDIVIDUAL CONTROL.

(a) ACCESS TO, AND CORRECTION, DELETION, AND PORTABILITY OF, COVERED DATA.—

(1) IN GENERAL.—Subject to paragraphs (2) and (3) and section 108, a covered entity shall provide an individual, immediately or as quickly as possible and in no case later than 90 days after receiving a verified request from the individual, with the right to reasonably—

(A) access—

(i) the covered data of the individual, or an accurate representation of the covered data of the individual, that is or has

been processed by the covered entity or any service provider on behalf of the covered entity;

(ii) if applicable, a list of categories of third parties and service providers to whom the covered entity has transferred the covered data of the individual; and

(iii) if a covered entity transfers covered data, a description of the purpose for which the covered entity transferred the covered data of the individual to a service provider or third party;

(B) request that the covered entity—

(i) correct inaccuracies or incomplete information with respect to the covered data of the individual that is maintained by the covered entity; and

(ii) notify any service provider or third party to which the covered entity transferred such covered data of the corrected information;

(C) request that the covered entity—

(i) either delete or deidentify covered data of the individual that is or has been maintained by the covered entity; and

(ii) notify any service provider or third party to which the covered entity transferred such covered data of the individual's request under clause (i), unless the transfer of such data to the third party was made at the direction of the individual; and

(D) to the extent that is technically feasible, provide covered data of the individual that is or has been generated and submitted to the covered entity by the individual and maintained by the covered entity in a portable, structured, and machine-readable format that is not subject to licensing restrictions.

(2) FREQUENCY AND COST OF ACCESS.—A covered entity shall—

(A) provide an individual with the opportunity to exercise the rights described in paragraph (1) not less than twice in any 12-month period; and

(B) with respect to the first 2 times that an individual exercises the rights described in paragraph (1) in any 12-month period, allow the individual to exercise such rights free of charge.

(3) EXCEPTIONS.—A covered entity—

(A) shall not comply with a request to exercise the rights described in paragraph (1) if the covered entity cannot verify—

(i) that the individual making the request is the individual to whom the covered data that is the subject of the request relates; or

(ii) the individual's assertion under paragraph (1)(B) that such information is inaccurate or incomplete;

(B) may decline to comply with a request that would—

(i) require the covered entity to retain any covered data for the sole purpose of fulfilling the request;

(ii) be impossible or demonstrably impracticable to comply with;

(iii) require the covered entity to combine, relink, or otherwise reidentify covered data that has been deidentified;

(iv) result in the release of trade secrets, or other proprietary or confidential data or business practices;

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

(vi) require disproportionate effort, taking into consideration available technology, or would not be reasonably feasible on technical grounds;

(vii) compromise the privacy, security, or other rights of the covered data of another individual;

(viii) be excessive or abusive to another individual; or

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

(C) may delete covered data instead of providing access and correction rights under subparagraphs (A) and (B) of paragraph (1) if such covered data—

(i) is not sensitive covered data; and

(ii) is used only for the purposes of contacting individuals with respect to marketing communications.

(b) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, establishing processes by which covered entities may verify requests to exercise rights described in subsection (a)(1).

SEC. 104. RIGHTS TO CONSENT.

(a) CONSENT.—Except as provided in section 108, a covered entity shall not, without the prior, affirmative express consent of an individual—

(1) transfer sensitive covered data of the individual to a third party; or

(2) process sensitive covered data of the individual.

(b) REQUIREMENTS FOR AFFIRMATIVE EXPRESS CONSENT.—In obtaining the affirmative express consent of an individual to process the sensitive covered data of the individual as required under subsection (a)(2), a covered entity shall provide the individual with notice that shall—

(1) include a clear description of the processing purpose for which the sensitive covered data will be processed;

(2) clearly identify any processing purpose that is necessary to fulfill a request made by the individual;

(3) include a prominent heading that would enable a reasonable individual to easily identify the processing purpose for which consent is sought; and

(4) clearly explain the individual's right to provide or withhold consent.

(c) 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 has actual knowledge that the individual is between 13 and 16 years of age.

(d) RIGHT TO OPT OUT.—Except as provided in section 108, a covered entity shall provide an individual with the ability to opt out of the collection, processing, or transfer of such individual's covered data before such collection, processing, or transfer occurs.

(e) PROHIBITION ON INFERRED CONSENT.—A covered entity shall not infer that an individual has provided affirmative express consent to a processing purpose from

the inaction of the individual or the individual's continued use of a service or product provided by the covered entity.

(f) WITHDRAWAL OF CONSENT.—A covered entity shall provide an individual with a clear and conspicuous means to withdraw affirmative express consent.

(g) RULEMAKING.—The Commission may promulgate regulations under section 553 of title 5, United States Code, to establish clear and conspicuous procedures for allowing individuals to provide or withdraw affirmative express consent for the collection of sensitive covered data.

SEC. 105. MINIMIZING DATA COLLECTION, PROCESSING, AND RETENTION.

(a) IN GENERAL.—Except as provided in section 108, a covered entity shall not collect, process, or transfer covered data beyond—

(1) what is reasonably necessary, proportionate, and limited to provide or improve a product, service, or a communication about a product or service, including what is reasonably necessary, proportionate, and limited to provide a product or service specifically requested by an individual or reasonably anticipated within the context of the covered entity's ongoing relationship with an individual;

(2) what is reasonably necessary, proportionate, or limited to otherwise process or transfer covered

data in a manner that is described in the privacy policy that the covered entity is required to publish under section 102(a); or

(3) what is expressly permitted by this Act or any other applicable Federal law.

(b) BEST PRACTICES.—Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidelines recommending best practices for covered entities to minimize the collection, processing, and transfer of covered data in accordance with this section.

(c) RULE OF CONSTRUCTION.—Notwithstanding section 404 of this Act, nothing in this section supersedes any other provision of this Act or other applicable Federal law.

SEC. 106. SERVICE PROVIDERS AND THIRD PARTIES.

(a) SERVICE PROVIDERS.—A service provider—

(1) shall not process service provider data for any processing purpose that is not performed on behalf of, and at the direction of, the covered entity that transferred the data to the service provider;

(2) shall not transfer service provider data to a third party for any purpose other than a purpose performed on behalf of, or at the direction of, the covered entity that transferred the data to the service provider;

(3) at the direction of the covered entity that transferred service provider data to the service provider, shall delete or deidentify such data—

(A) as soon as practicable after the service provider has completed providing the service or function for which the data was transferred to the service provider; or

(B) as soon as practicable after the end of the period during which the service provider is to provide services with respect to such data, as agreed to by the service provider and the covered entity that transferred the data;

(4) is exempt from the requirements of section 103 with respect to service provider data, but shall, to the extent practicable—

(A) assist the covered entity from which it received the service provider data in fulfilling requests to exercise rights under section 103(a); and

(B) upon receiving notice from a covered entity of a verified request made under section 103(a)(1) to delete, deidentify, or correct service provider data held by the service provider, delete, deidentify, or correct such data; and

(5) is exempt from the requirements of sections 104 and 105.

(b) THIRD PARTIES.—A third party—

(1) shall not process third party data for a processing purpose inconsistent with the reasonable expectation of the individual to whom such data relates;

(2) for purposes of paragraph (1), may reasonably rely on representations made by the covered entity that transferred third party data regarding the reasonable expectations of individuals to whom such data relates, 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) is exempt from the requirements of sections 104 and 105.

(c) BANKRUPTCY.—In the event that a covered entity enters into a bankruptcy proceeding which would lead to the disclosure of covered data to a third party, the covered entity shall in a reasonable time prior to the disclosure—

(1) provide notice of the proposed disclosure of covered data, including the name of the third party and its policies and practices with respect to the covered data, to all affected individuals; and

(2) provide each affected individual with the opportunity to withdraw any previous affirmative express consent related to the covered data of the individual or request the deletion or deidentification of the covered data of the individual.

(d) ADDITIONAL OBLIGATIONS ON COVERED ENTITIES.—

(1) IN GENERAL.—A covered entity shall exercise reasonable due diligence to ensure compliance with this section before—

(A) selecting a service provider; or

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

(2) GUIDANCE.—Not later than 2 years after the effective date of this Act, the Commission shall publish guidance regarding compliance with this subsection. Such guidance shall, to the extent practicable, minimize unreasonable burdens on small- and medium-sized covered entities.

SEC. 107. PRIVACY IMPACT ASSESSMENTS.

(a) PRIVACY IMPACT ASSESSMENTS OF NEW OR MATERIAL CHANGES TO PROCESSING OF COVERED DATA.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act (or, if later, not later than 1 year after a covered entity first meets

the definition of a large data holder (as defined in section 2)), each covered entity that is a large data holder shall conduct a privacy impact assessment of each of its processing activities involving covered data that present a heightened risk of harm to individuals, and each such assessment shall weigh the benefits of the covered entity's covered data collection, processing, and transfer practices against the potential adverse consequences to individual privacy of such practices.

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

(A) shall be reasonable and appropriate in scope given—

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

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

(iii) the size of the covered entity; and

(iv) the potential risks posed to the privacy of individuals by the collection, processing, or transfer of covered data by the covered entity;

(B) shall be documented in written form and maintained by the covered entity unless rendered out of date by a subsequent assessment conducted under subsection (b); and

(C) shall be approved by the data privacy officer of the covered entity.

(b) ONGOING PRIVACY IMPACT ASSESSMENTS.—

(1) IN GENERAL.—A covered entity that is a large data holder shall, not less frequently than once every 2 years after the covered entity conducted the privacy impact assessment required under subsection (a), conduct a privacy impact assessment of the collection, processing, and transfer of covered data by the covered entity to assess the extent to which—

(A) the ongoing practices of the covered entity are consistent with the covered entity's published privacy policies;

(B) any customizable privacy settings included in a service or product offered by the covered entity are adequately accessible to individuals who use the service or product and are effective in meeting the privacy preferences of such individuals;

(C) the practices and privacy settings described in subparagraphs (A) and (B), respectively—

(i) meet the expectations of a reasonable individual; and

(ii) provide an individual with adequate control over the individual's covered data;

(D) the covered entity could enhance the privacy and security of covered data through technical or operational safeguards such as encryption, deidentification, and other privacy-enhancing technologies; and

(E) the processing of covered data is compatible with the stated purposes for which it was collected.

(2) APPROVAL BY DATA PRIVACY OFFICER.—The data privacy officer of a covered entity shall approve the findings of an assessment conducted by the covered entity under this subsection.

SEC. 108. SCOPE OF COVERAGE.

(a) GENERAL EXCEPTIONS.—Notwithstanding any provision of this title other than subsections (a) through (c) of section 102, a covered entity may collect, process or transfer covered data for any of the following purposes,

provided that the collection, processing, or transfer is reasonably necessary, proportionate, and limited to such purpose:

(1) To initiate or complete a transaction or to fulfill an order or provide a service specifically requested by an individual, including associated routine administrative activities such as billing, shipping, financial reporting, and accounting.

(2) To perform internal system maintenance, diagnostics, product or service management, inventory management, and network management.

(3) To prevent, detect, or respond to a security incident or trespassing, provide a secure environment, or maintain the safety and security of a product, service, network, or individual.

(4) To protect against malicious, deceptive, fraudulent, or illegal activity.

(5) To comply with a legal obligation or the establishment, exercise, analysis, or defense of legal claims or rights, or as required or specifically authorized by law.

(6) To comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by an Executive agency.

(7) To cooperate with an Executive agency or a law enforcement official acting under the authority of an Executive or State agency concerning conduct or activity that the Executive agency or law enforcement official reasonably and in good faith believes may violate Federal, State, or local law, or pose a threat to public safety or national security.

(8) To address risks to the safety of an individual or group of individuals, or to ensure customer safety, including by authenticating individuals in order to provide access to large venues open to the public.

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

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

(A) is in the public interest;

(B) adheres to all applicable ethics and privacy laws; and

(C) is approved, monitored, and governed by an institutional review board or other oversight entity that meets standards promulgated by the Commission pursuant to section 553 of title 5, United States Code.

(11) To transfer covered data to a service provider.

(12) For a purpose identified by the Commission pursuant to a regulation promulgated under subsection (b).

(b) ADDITIONAL PURPOSES.—The Commission may promulgate regulations under section 553 of title 5, United States Code, identifying additional purposes for which a covered entity may collect, process or transfer covered data.

(c) SMALL BUSINESS EXCEPTION.—Sections 103, 105, and 301 shall not apply in the case of a covered entity that can establish that, for 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)—

(1) the covered entity's average annual gross revenues did not exceed $50,000,000;

(2) on average, the covered entity annually processed the covered data of less than 1,000,000 individuals;

(3) the covered entity never employed more than 500 individuals at any one time; and

(4) the covered entity derived less than 50 percent of its revenues from transferring covered data.

TITLE II—DATA TRANSPARENCY, INTEGRITY, AND SECURITY

SEC. 201. CIVIL RIGHTS, ALGORITHM BIAS, DETECTION, AND MITIGATION.

(a) CIVIL RIGHTS PROTECTIONS.—A covered entity, service provider, or third party may not collect, process, or transfer covered data in violation of Federal civil rights laws.

(b) FTC ENFORCEMENT ASSISTANCE.—

(1) IN GENERAL.—Whenever the Commission obtains information that a covered entity may have processed or transferred covered data in violation of Federal civil rights laws, the Commission shall transmit such information (excluding any such information that is a trade secret as defined by section 1839 of title 18, United States Code) to the appropriate Executive agency or State agency with authority to initiate proceedings relating to such violation.

(2) ANNUAL REPORT.—Beginning in 2022, the Commission shall submit an annual report to Congress that includes—

(A) a summary of the types of information the Commission transmitted to Executive agen-

cies or State agencies during the preceding year pursuant to this subsection; and

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

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

(4) RELATIONSHIP TO OTHER LAWS.—Notwithstanding section 404, nothing in this subsection shall supersede any other provision of law.

(c) ALGORITHM TRANSPARENCY REPORTS.—

(1) STUDY AND REPORT.—

(A) STUDY.—The Commission shall conduct a study, using the Commission's authority under section 6(b) of the Federal Trade Commission Act (15 U.S.C. 46(b)), examining the use of algorithms to process covered data in a manner that may violate Federal anti-discrimination laws.

(B) REPORT.—Not later than 3 years after the date of enactment of this Act, the Commission shall publish a report containing the results of the study required under subparagraph (A).

(C) GUIDANCE.—The Commission shall use the results of the study described in subparagraph (A) to develop guidance to assist covered entities in avoiding the use of algorithms to process covered data in a manner that violates Federal civil rights laws.

(2) UPDATED REPORT.—Not later than 5 years after the publication of the report required under paragraph (1), the Commission shall publish an updated report.

SEC. 202. DATA BROKERS.

(a) IN GENERAL.—Not later than January 31 of each calendar year that follows a calendar year during which a covered entity acted as a data broker, such covered entity shall register with the Commission pursuant to the requirements of this section.

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

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

(2) Provide the Commission with the following information:

(A) The name and primary physical, email, and internet addresses of the data broker.

(B) Any additional information or explanation the data broker chooses to provide concerning its data collection and processing practices.

(c) PENALTIES.—A data broker that fails to register as required under subsection (a) shall be liable for—

(1) a civil penalty of $50 for each day it fails to register, not to exceed a total of $10,000 for each year; and

(2) an amount equal to the fees due under this section for each year that it failed to register as required under subsection (a).

(d) PUBLICATION OF REGISTRATION INFORMATION.—The Commission shall publish on the internet website of the Commission the registration information provided by data brokers under this section.

SEC. 203. PROTECTION OF COVERED DATA.

(a) IN GENERAL.—A covered entity shall establish, implement, and maintain reasonable administrative, technical, and physical data security policies and practices to protect against risks to the confidentiality, security, and integrity of covered data.

(b) DATA SECURITY REQUIREMENTS.—The data security policies and practices required under subsection (a) shall be—

(1) appropriate to the size and complexity of the covered entity, the nature and scope of the covered entity's collection or processing of covered data, the volume and nature of the covered data at issue, and the cost of available tools to improve security and reduce vulnerabilities; and

(2) designed to—

(A) identify and assess vulnerabilities to covered data;

(B) take reasonable preventative and corrective action to address known vulnerabilities to covered data; and

(C) detect, respond to, and recover from cybersecurity incidents related to covered data.

(c) RULEMAKING AND GUIDANCE.—

(1) RULEMAKING AUTHORITY AND SCOPE.—

(A) IN GENERAL.—The Commission may, pursuant to a proceeding in accordance with section 553 of title 5, United States Code, issue regulations to identify processes for receiving and assessing information regarding vulnerabilities to covered data that are reported to the covered entity.

(B) CONSULTATION WITH NIST.—In promulgating regulations under this paragraph, the

Commission shall consult with, and take into consideration guidance from, the National Institute for Standards and Technology.

(2) GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance to covered entities on how to—

(A) identify and assess vulnerabilities to covered data, including—

(i) the potential for unauthorized access to covered data;

(ii) vulnerabilities in the covered entity's collection or processing of covered data;

(iii) the management of access rights; and

(iv) the use of service providers to process covered data;

(B) take reasonable preventative and corrective action to address vulnerabilities to covered data; and

(C) detect, respond to, and recover from cybersecurity incidents and events.

(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, shall be deemed to be in compliance with the requirements of this section with respect to covered data that is subject to the requirements of such Act.

TITLE III—CORPORATE ACCOUNTABILITY

SEC. 301. DESIGNATION OF DATA PRIVACY OFFICER AND DATA SECURITY OFFICER.

(a) IN GENERAL.—A covered entity shall designate—

(1) 1 or more qualified employees or contractors as a data privacy officer; and

(2) 1 or more qualified employees or contractors (in addition to any employee or contractor designated under paragraph (1)) as a data security officer.

(b) RESPONSIBILITIES OF DATA PRIVACY OFFICERS AND DATA SECURITY OFFICERS.—An employee or contractor who is designated by a covered entity as a data privacy officer or a data security officer shall be responsible for, at a minimum, coordinating the covered entity's policies and practices regarding—

(1) in the case of a data privacy officer, compliance with the privacy requirements with respect to covered data under this Act; and

(2) in the case of a data security officer, the security requirements with respect to covered data under this Act.

SEC. 302. INTERNAL CONTROLS.

A covered entity shall maintain internal controls and reporting structures to ensure that appropriate senior management officials of the covered entity are involved in assessing risks and making decisions that implicate compliance with this Act.

SEC. 303. WHISTLEBLOWER PROTECTIONS.

(a) DEFINITIONS.—For purposes of this section:

(1) WHISTLEBLOWER.—The term ''whistleblower'' means any employee or contractor of a covered entity who voluntarily provides to the Commission original information relating to non-compliance with, or any violation or alleged violation of, this Act or any regulation promulgated under this Act.

(2) ORIGINAL INFORMATION.—The term ''original information'' means information that is provided to the Commission by an individual and—

(A) is derived from the independent knowledge or analysis of an individual;

(B) is not known to the Commission from any other source at the time the individual provides the information; and

(C) is not exclusively derived from an allegation made in a judicial or an administrative action, in a governmental report, a hearing, an audit, or an investigation, or from news media, unless the individual is a source of the allegation.

(b) EFFECT OF WHISTLEBLOWER RETALIATIONS ON PENALTIES.—In seeking penalties under section 401 for a violation of this Act or a regulation promulgated under this Act by a covered entity, the Commission shall consider whether the covered entity retaliated against an individual who was a whistleblower with respect to original information that led to the successful resolution of an administrative or judicial action brought by the Commission or the Attorney General of the United States on behalf of the Commission under this Act against such covered entity.

TITLE IV—ENFORCEMENT AUTHORITY AND NEW PROGRAMS

SEC. 401. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) 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)).

(b) POWERS OF COMMISSION.—

(1) IN GENERAL.—Except as provided in subsections (c) and (d), 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.

(2) 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; AUTHORITY PRESERVED.—The Commission shall not bring any action to enforce the prohibition in section 5 of the Federal Trade Commission Act (15 U.S.C. 45) on unfair or deceptive acts or practices with respect to the privacy or security of covered data, unless such alleged act of practice violates this Act.

(c) COMMON CARRIERS AND NONPROFIT ORGANIZATIONS.—Notwithstanding section 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46) or any jurisdictional limitation of the Commission, the Commission shall also enforce this Act and the regulations promulgated under this Act, in the same manner provided in subsections (a) and (b) of this subsection, with respect to—

(1) 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

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

(d) DATA PRIVACY AND SECURITY FUND.—

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

(2) DEPOSITS.—

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

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

(3) USE OF FUND AMOUNTS.—Amounts in the Victims Relief Fund shall be available to the Commission, without fiscal year limitation, to provide re-

dress, payments or compensation, or other monetary relief to individuals harmed by an act or practice for which civil penalties have been imposed under this Act. 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 consumer or business education relating to data privacy and security or for the purpose of engaging in technological research that the Commission considers necessary to enforce this Act.

(4) AMOUNTS NOT SUBJECT TO APPORTIONMENT.—Notwithstanding any other provision of law, amounts in the Victims Relief Fund shall not be subject to apportionment for purposes of chapter 15 of title 31, United States Code, or under any other authority.

(e) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Commission $100,000,000 to carry out this Act.

SEC. 402. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) CIVIL ACTION.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is adversely affected by the engagement of any covered entity in an

act or practice that violates this Act or a regulation promulgated under this Act, the attorney general of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate 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) obtain such other relief as the court may consider to be appropriate.

(b) RIGHTS OF THE COMMISSION.—

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

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

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

(2) NOTIFICATION TIMELINE.—Where it is not feasible for the attorney general of a State to provide the notification required by paragraph (2) before initiating a civil action under paragraph (1), the attorney general shall notify the Commission immediately after initiating the civil action.

(c) CONSOLIDATION OF ACTIONS BROUGHT BY TWO OR MORE STATE ATTORNEYS GENERAL.—Whenever a civil action under subsection (a) is pending and another civil action or actions are commenced pursuant to such subsection in a different Federal district court or courts that involve 1 or more common questions of fact, a defendant in such action or actions my request that such action or actions be transferred for the purposes of consolidated pretrial proceedings and trial to the United States District Court for the District of Columbia; provided however, that no such action shall be transferred if pretrial proceedings in that action have been concluded before a subsequent action is filed by the attorney general of the State.

(d) ACTIONS BY 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 of a State may, during

the pendency of such action, institute a civil action against any defendant named in the complaint in the action instituted by or on behalf of the Commission for violation of this Act or a regulation promulgated under this Act that is alleged in such complaint.

(e) INVESTIGATORY POWERS.—Nothing in this section shall be construed to prevent the attorney general of a State or another authorized official of a State from exercising the powers conferred on the attorney general or the State official by the laws of the State to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

(f) VENUE; SERVICE OF PROCESS.—

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

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

(A) is an inhabitant; or

(B) may be found.

(g) ACTIONS BY OTHER STATE OFFICIALS.—Any State official who is authorized by the State attorney general to be the exclusive authority in that State to enforce this Act may bring a civil action under subsection (a), subject to the same requirements and limitations that apply under this section to civil actions brought under such subsection by State attorneys general.

SEC. 403. APPROVED CERTIFICATION PROGRAMS.

(a) IN GENERAL.—The Commission shall establish a program in which the Commission shall approve voluntary consensus standards or certification programs that covered entities may use to comply with 1 or more provisions in this Act.

(b) EFFECT OF APPROVAL.—A covered entity in compliance with a voluntary consensus standard approved by the Commission shall be deemed to be in compliance with the provisions of this Act.

(c) TIME FOR APPROVAL.—The Commission shall issue a decision regarding the approval of a proposed voluntary consensus standard not later than 180 days after a request for approval is submitted.

(d) EFFECT OF NON-COMPLIANCE.—A covered entity that claims compliance with an approved voluntary consensus standard and is found not to be in compliance with

such program by the Commission or in any judicial proceeding shall be considered to be in violation of this Act.

(e) RULEMAKING.—Not later than 120 days after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, establishing a process for review of requests for approval of proposed voluntary consensus standards under this section.

(f) REQUIREMENTS.—To be eligible for approval by the Commission, a voluntary consensus standard shall meet the requirements for voluntary consensus standards set forth in Office of Management and Budget Circular A–119, or other equivalent guidance document, ensuring that they are the result of due process procedures and appropriately balance the interests of all the stakeholders, including individuals, businesses, organizations, and other entities making lawful uses of the covered data covered by the standard, and—

(1) specify clear and enforceable requirements for covered entities participating in the program that provide an overall level of data privacy or data security protection that is equivalent to or greater than that provided in the relevant provisions in this Act;

(2) require each participating covered entity to post in a prominent place a clear and conspicuous

public attestation of compliance and a link to the website described in paragraph (4);

(3) include a process for an independent assessment of a participating covered entity's compliance with the voluntary consensus standard or certification program prior to certification and at reasonable intervals thereafter;

(4) create a website describing the voluntary consensus standard or certification program's goals and requirements, listing participating covered entities, and providing a method for individuals to ask questions and file complaints about the program or any participating covered entity;

(5) take meaningful action for non-compliance with the relevant provisions of this Act by any participating covered entity, which shall depend on the severity of the non-compliance and may include—

(A) removing the covered entity from the program;

(B) referring the covered entity to the Commission or other appropriate Federal or State agencies for enforcement;

(C) publicly reporting the disciplinary action taken with respect to the covered entity;

(D) providing redress to individuals harmed by the non-compliance;

(E) making voluntary payments to the United States Treasury; and

(F) taking any other action or actions to ensure the compliance of the covered entity with respect to the relevant provisions of this Act; and

(6) issue annual reports to the Commission and to the public detailing the activities of the program and its effectiveness during the preceding year in ensuring compliance with the relevant provisions of this Act by participating covered entities and taking meaningful disciplinary action for non-compliance with such provisions by such entities.

SEC. 404. RELATIONSHIP BETWEEN FEDERAL AND STATE LAW.

(a) RELATIONSHIP TO STATE LAW.—No State or political subdivision of a State may adopt, maintain, enforce, or continue in effect any law, regulation, rule, requirement, or standard related to the data privacy or data security and associated activities of covered entities.

(b) SAVINGS PROVISION.—Subsection (a) may not be construed to preempt State laws that directly establish re-

quirements for the notification of consumers in the event of a data breach.

(c) RELATIONSHIP TO OTHER FEDERAL LAWS.—

(1) IN GENERAL.—Except as provided in paragraphs (2) and (3), the requirements of this Act shall supersede any other Federal law or regulation relating to the privacy or security of covered data or associated activities of covered entities.

(2) SAVINGS PROVISION.—This Act may not be construed to modify, limit, or supersede the operation of the following:

(A) The Children's Online Privacy Protection Act (15 U.S.C. 6501 et seq.).

(B) The Communications Assistance for Law Enforcement Act (47 U.S.C. 1001 et seq.).

(C) Section 227 of the Communications Act of 1934 (47 U.S.C. 227).

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

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

(F) The Health Insurance Portability and Accountability Act (Public Law 104–191).

(G) The Electronic Communications Privacy Act (18 U.S.C. 2510 et seq.).

(H) Section 444 of the General Education Provisions Act (20 U.S.C. 1232g) (commonly referred to as the ''Family Educational Rights and Privacy Act of 1974'').

(I) The Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et seq.).

(J) The Federal Aviation Act of 1958 (49 U.S.C. App. 1301 et seq.).

(K) The Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.).

(3) COMPLIANCE WITH SAVED FEDERAL LAWS.—To the extent that the data collection, processing, or transfer activities of a covered entity are subject to a law listed in paragraph (2), such activities of such entity shall not be subject to the requirements of this Act.

(4) NONAPPLICATION OF FCC LAWS AND REGULATIONS TO COVERED ENTITIES.—Notwithstanding any other provision of law, neither any provision of the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof and supplementary thereto nor any regulation promulgated by the Federal Communications Commission under such Acts shall apply to any covered entity with re-

spect to the collection, use, processing, transferring, or security of individual information, except to the extent that such provision or regulation pertains solely to ''911'' lines or other emergency line of a hospital, medical provider or service office, health care facility, poison control center, fire protection agency, or law enforcement agency.

SEC. 405. CONSTITUTIONAL AVOIDANCE.

The provisions of this Act shall be construed, to the greatest extent possible, to avoid conflicting with the Constitution of the United States, including the protections of free speech and freedom of the press established under the First Amendment to the Constitution of the United States.

SEC. 406. SEVERABILITY.

If any provision of this Act, or an amendment made by this Act, is determined to be unenforceable or invalid, the remaining provisions of this Act and the amendments made by this Act shall not be affected.

○