117TH CONGRESS
1ST SESSION

S. 1494

To protect the privacy of consumers.

IN THE SENATE OF THE UNITED STATES

APRIL 29, 2021

Mr. MORAN introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To protect the privacy of consumers.

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 ''Consumer Data Privacy and Security Act of 2021''.

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

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.
Sec. 3. Collection and processing of personal data.
Sec. 4. Right to know.
Sec. 5. Individual control.
Sec. 6. Security.
Sec. 7. Accountability.
Sec. 8. Rules relating to service providers.
Sec. 9. Enforcement.
Sec. 10. Relation to other laws.

Sec. 11. Commission resources.
Sec. 12. Guidance and reporting.
Sec. 13. Severability.
Sec. 14. Effective date.

SEC. 2. DEFINITIONS.

In this Act:

(1) BIOMETRIC INFORMATION.—The term ''biometric information'' means information, resulting from specific technical processing related to the physical, biological, physiological, genetic, or behavioral characteristics of an individual, that identifies the individual.

(2) COLLECTION.—The term ''collection'' means acquiring personal data by any means, including by receiving, purchasing, or leasing the data or by observing or interacting with the individual to whom the data relates.

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

(4) COVERED ENTITY.—

(A) IN GENERAL.—The term ''covered entity'' means any entity that—

(i) alone, or jointly with others, determines the purpose and means of collecting or processing personal data; and

(ii) is—

(I) a person over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2));

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

(III) a nonprofit organization, including any organization that is not organized to carry on business for its own profit or that of its members.

(B) LIMITATION.—An entity shall not be considered to be a covered entity with respect to personal data to the extent that the entity is a service provider with respect to such data.

(5) DE-IDENTIFY.—The term ''de-identify'' means, with respect to personal data held by a covered entity or service provider, that the covered entity or service provider—

(A) alters, anonymizes, or aggregates the data so that there is a reasonable basis for expecting that the data could not be linked (in-

cluding by the entity or service provider) as a practical matter to a specific individual;

(B) publicly commits to refrain from attempting to re-identify the data with a specific individual, and adopts controls to prevent such identification; and

(C) causes the data to be covered by a contractual or other legally enforceable prohibition on each entity to which the covered entity or service provider discloses the data from attempting to use the data to identify a specific individual and requires the same of all onward disclosures.

(6) DELETE.—The term ''delete'' means to remove or destroy information such that the information is not able to be retrieved in the ordinary course of business.

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

(8) MATERIAL CHANGE.—The term ''material change'' means a change to a policy or practice of a covered entity or service provider that—

(A) relates to the collection or processing of personal data by the covered entity or service provider;

(B) is likely to affect the conduct or decision of a reasonable individual with respect to any personal data of the individual that is subject to such policy or practice; and

(C) in the case of a service provider, is made at the direction of the covered entity on whose behalf the service provider is performing a service or function.

(9) PERSONAL DATA.—

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

(B) LINKED OR REASONABLY LINKABLE.—

(i) IN GENERAL.—For purposes of subparagraph (A), information held by a covered entity or service provider is linked or reasonably linkable to a specific individual if it can be used on its own or in combination with other information held by, or readily accessible to, the covered entity or service provider to identify the individual.

(ii) APPLICATION TO DEVICE-LEVEL IDENTIFIERS.—A persistent identifier that

is used to identify a specific individual over time and across services and platforms, including a customer number held in a cookie, a static Internet Protocol (IP) address, a processor or device serial number, or another unique device identifier, shall be considered information that is linked or reasonably linkable to the individual for purposes of subparagraph (A).

(C) EXCLUSION.—The term ''personal data'' does not include—

(i) de-identified data;

(ii) data that has been rendered unreadable or indecipherable;

(iii) information about employees or employment status collected or used by an employer pursuant to an employer-employee relationship, including information related to prospective employees and relevant application materials;

(iv) publicly available information;

(v) data that has undergone pseudonymization; or

(vi) employee data.

(D) EMPLOYEE DATA.—For purposes of subparagraph (C), the term ''employee data'' means information collected by a covered entity or the service provider of a covered entity that is—

(i) contact information for an individual or the individual's emergency contact that is collected in the course of the individual's employment or application for employment (including on a contract or temporary basis) with the covered entity, provided that such information is retained or processed by the covered entity or service provider solely for purposes related to the individual's employment or application for employment with the covered entity; or

(ii) information about an individual who is an employee or former employee of the covered entity (or a relative of such an individual) that is necessary to administer benefits to which such individual or relative is entitled on the basis of the individual's employment with the covered entity, provided that such data is retained or processed by the covered entity or service

provider solely for the purpose of administering such benefits.

(10) PSEUDONYMIZATION.—The term ''pseudonymization'' means the processing of personal data so that the personal data can no longer be attributed or reasonably linked to a specific individual without the use of additional information, provided that such additional information—

(A) is kept separately; and

(B) is subject to technical and organizational measures to ensure that the personal data is not attributed to a specific individual.

(11) PRIVACY OFFICER.—The term ''privacy officer'' means an individual designated by a covered entity or service provider under section 7(b)(1) to be the privacy officer of the covered entity.

(12) PROCESSING.—The term ''processing'' means any operation or set of operations performed on personal data, including the analysis, organization, structuring, retaining, using, disclosing, transmitting, sharing, transferring, selling, licensing, or otherwise handling of personal data.

(13) PUBLICLY AVAILABLE INFORMATION.—

(A) IN GENERAL.—The term ''publicly available information'' means any information

that a covered entity or service provider has a reasonable basis to believe is lawfully made available to the general public from—

(i) a Federal, State, or local government record;

(ii) widely distributed media; or

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

(B) REASONABLE BASIS TO BELIEVE.—For purposes of subparagraph (A), reasonable bases for believing that information is lawfully made available to the general public shall include a written determination by a covered entity or service provider that the information is of a type that is lawfully made available to the general public.

(14) SENSITIVE PERSONAL DATA.—The term ''sensitive personal data'' means personal data that is—

(A) a unique, government-issued identifier, such as a social security number, passport number, driver's license number, or taxpayer identification number;

(B) a user name or email address in combination with a password or security question and answer that would permit access to an online account;

(C) biometric information of an individual;

(D) the content of a wire communication, oral communication, or electronic communication, as those terms are defined in section 2510 of title 18, United States Code, to which the individual is a party, unless the covered entity is the intended recipient of the communication;

(E) information that relates to—

(i) the past, present, or future diagnosed physical or mental health or condition of an individual;

(ii) the provision of health care to an individual; or

(iii) the past, present, or future payment for the provision of health care to an individual;

(F) a financial account number, debit card number, credit card number, if combined with an access code, password, or credentials that provide access to such an account;

(G) the race or ethnicity of the individual;

(H) the religious beliefs or affiliation of the individual;

(I) the sexual orientation of the individual;

(J) the precise geolocation of an individual that is technically derived and that is capable of determining with reasonable specificity the past or present actual physical location of the individual more precisely than a zip code, street, or town or city level; or

(K) such other specific categories of personal data as the Commission may define by rule issued in accordance with section 553 of title 5, United States Code, the collection or processing of which could lead to reasonably foreseeable harm to an individual.

(15) SERVICE PROVIDER.—The term ''service provider'' means an entity that collects or processes personal data on behalf of, and at the direction of, a covered entity to which the service provider is unaffiliated, but only—

(A) with respect to the personal data collected or processed on the behalf of, and at the direction of, such covered entity; and

(B) to the extent that the collection or processing—

(i) is on the behalf of, and at the direction of, such covered entity; or

(ii) is permitted under section 3(c).

(16) SMALL BUSINESS.—The term ''small business'' means any covered entity or service provider that—

(A) for the most recent 6-month period—

(i) employs not more than 500 employees; and

(ii) maintains less than $50,000,000 in average gross receipts for the previous 3 years; and

(B) collects or processes on an annual basis—

(i) the personal data of fewer than 1,000,000 individuals; or

(ii) the sensitive personal data of fewer than 100,000 individuals.

(17) THIRD PARTY.—

(A) IN GENERAL.—The term ''third party'' means a covered entity that receives third party personal data from an unaffiliated covered entity, but only with respect to such third party personal data.

(B) THIRD PARTY PERSONAL DATA.—For purposes of subparagraph (A), the term ''third party personal data'' means personal data that a covered entity discloses to another unaffiliated covered entity and such disclosure—

(i) is not directed by the individual to whom the personal data relates; and

(ii) is not necessary to complete a transaction or fulfill a request made by the individual to whom such data relates.

(18) UNAFFILIATED.—The term ''unaffiliated'' means, with respect to two or more entities, that the entities do not share interrelated operations, common management, centralized control of labor relations, or common ownership or financial control.

SEC. 3. COLLECTION AND PROCESSING OF PERSONAL DATA.

(a) REQUIREMENTS.—

(1) IN GENERAL.—Except as provided in paragraphs (2) and (3), a covered entity shall not collect or process personal data of an individual unless—

(A) the individual has consented explicitly or implicitly to such collection or processing for a specific purpose, in accordance with subsection (b); or

(B) the covered entity collects or processes the personal data in accordance with a permissible purpose described in subsection (c).

(2) APPLICATION TO THIRD PARTIES.—

(A) IN GENERAL.—A covered entity that is a third party with respect to the personal data of an individual may collect or process such personal data without directly obtaining the individual's consent as required under paragraph (1)(A) if—

(i) the covered entity from whom the third party received the personal data of the individual involved—

(I) has provided the individual with notice of—

(aa) the fact that the covered entity would disclose the individual's personal data to the third party; and

(bb) the purposes for which the third party will collect or process the personal data of the individual; and

(II) the individual has consented to such disclosure and such collection

or processing of the individual's personal data; or

(ii) the third party collects or process the personal data in accordance with a permissible purpose described in subsection (c).

(B) NOTICE AND CONSENT REQUIREMENT FOR DIFFERENT OR ADDITIONAL COLLECTION OR PROCESSING.—A covered entity that is a third party with respect to the personal data of an individual shall obtain the consent of such individual in accordance with subsection (b) before collecting or processing such personal data if the specific purpose for such collection or processing—

(i) is not a purpose described in paragraph (1), (2), (4), or (6) of subsection (c); and

(ii) is different from, or in addition to, the purpose for any collection or processing to which the individual previously consented in accordance with subsection (b).

(C) DUTY TO EXERCISE REASONABLE DUE DILIGENCE PRIOR TO RELIANCE ON COVERED ENTITY REPRESENTATIONS.—For purposes of

subparagraph (A), a covered entity that is a third party with respect to the personal data of an individual may reasonably rely on representations made by the covered entity from whom the third party received such data regarding the notice provided to, and the consent obtained from, such individual, provided that the third party has determined, after exercising reasonable due diligence, that the covered entity is credible.

(3) NOTICE AND CONSENT OBTAINED BY SERVICE PROVIDERS.—A service provider may provide notice to, and obtain consent from, an individual in accordance with subsection (b) on behalf of a covered entity.

(b) CONSENT.—

(1) IN GENERAL.—

(A) IMPLICIT CONSENT.—Except as provided in subparagraph (B), an individual shall be deemed to have consented to a request to collect or process the individual's personal data if the individual fails to decline the request after being provided with the notice described in paragraph (2) and a reasonable amount of time to respond to the request.

(B) EXPRESS AFFIRMATIVE CONSENT REQUIREMENT.—

(i) IN GENERAL.—The express affirmative consent of an individual is required to collect or process the personal data of the individual if the collection or processing—

(I) involves sensitive personal data of the individual; or

(II) involves the disclosure of personal data to a third party for a purpose that is not described in subsection (c).

(ii) REQUIREMENTS FOR VALID EXPRESS AFFIRMATIVE CONSENT.—For purposes of clause (i), the express affirmative consent of an individual to a request to collect or process the personal data of the individual—

(I) shall be clearly, prominently, and unmistakably stated;

(II) shall be provided in response to a request that includes the notice described in paragraph (2); and

(III) cannot be inferred from inaction.

(2) NOTICE REQUIRED.—

(A) IN GENERAL.—In requesting the consent of an individual to collect or process the individual's personal data, a covered entity shall provide the individual with notice, in a concise, meaningful, timely, prominent, and easy-to-understand format, that includes—

(i) the types of personal data collected and processed;

(ii) a description of the purposes for which the covered entity seeks to collect or process that individual's personal data; and

(iii) the information described in subparagraph (B).

(B) CONTENTS.—The notice provided by a covered entity under subparagraph (A) shall include—

(i) information on how the individual may access the privacy policy of the covered entity described in section 4(a);

(ii) information on how the individual may exercise the rights provided for under this Act; and

(iii) notice of whether the collection or processing by the covered entity—

(I) includes the disclosure of personal data to third parties; or

(II) involves sensitive personal data.

(C) SEPARATION.—If consent is obtained in the context of a notice that also concerns matters other than the collection or processing of personal data, the request for consent shall be presented in a manner that is clearly distinguishable from the other matters.

(3) WITHDRAWAL OF CONSENT.—

(A) IN GENERAL.—A covered entity shall provide an individual with the means to withdraw previously given consent to collect or process the personal data of the individual—

(i) at any time and place that is reasonably practicable; and

(ii) in a manner that is as accessible as reasonably practicable.

(B) EFFECT.—A withdrawal made under subparagraph (A)—

(i) shall take effect without undue delay;

(ii) shall remain in effect until the individual revokes or limits that denial or withdrawal; and

(iii) shall not apply to any collection or processing of personal data that occurred before the date on which the withdrawal is made.

(c) PERMISSIBLE PURPOSES.—A covered entity or service provider may collect or process the personal data of an individual without consent to the extent that such collection or processing is reasonably necessary and limited to the following purposes (except that a covered entity that is a third party with respect to personal data may not collect or process such data without consent for the purposes described in paragraphs (3), (5), and (6)):

(1) PROVISION OF SERVICE OR PERFORMANCE OF A CONTRACT.—To—

(A) provide a service, perform a contract, or conduct a transaction that the individual has initiated; or

(B) take steps in furtherance of the request initiated by the individual prior to providing the service or entering into a contract or transaction.

(2) COMPLIANCE WITH LAWS.—To comply with a Federal, State, or local law or another applicable legal requirement, including a subpoena, summons, or other properly executed compulsory process, or to exercise or defend a legal claim, as specifically authorized by law.

(3) IMMEDIATE DANGER.—To prevent imminent danger to the personal safety of any individual, including by effectuating a product recall pursuant to Federal or State law.

(4) FRAUD PREVENTION AND PROTECTION OF SECURITY.—To protect the rights, property, services, or information systems of the covered entity or service provider, or any individual, including to investigate a possible crime or to protect against security threats, abuse, malicious conduct, deception, fraud, theft, unauthorized transactions, or any other unlawful activity.

(5) RESEARCH.—In the case of a covered entity only, to conduct research that—

(A) is performed for the primary purpose of advancing a broadly recognized public interest;

(B) is performed by the covered entity (or by a service provider at the direction of the cov-

ered entity) and is not disclosed to any third party;

(C) is broadly compatible with the purposes for which the data was originally collected or processed; and

(D) adheres to all applicable ethics and privacy laws.

(6) OPERATIONAL PURPOSES.—To—

(A) perform internal operations or analytics for a product or service offered by the covered entity or service provider, such as billing, shipping, internal systems maintenance, diagnostics, inventory management, financial reporting or accounting, serving an internet website, or network management;

(B) use on a short-term, transient basis, provided that the personal data—

(i) is not disclosed to a third party; and

(ii) is not used to build a persistent profile of the individual;

(C) in the case of a covered entity only, market or advertise a service or product to an individual if the personal data used for the marketing or advertising was collected directly

from the individual by the covered entity or by a service provider on behalf of the covered entity;

(D) improve a product, service, or activity used, requested, or authorized by the individual, including analytics, forecasting, the repair of errors that impair existing intended functionality, actions to verify or maintain quality or safety of the product, service, or activity, or the ongoing provision of customer service and support by the covered entity or service provider; or

(E) other additional specific categories of operational purposes that the Commission may define by rule, issued in accordance with section 553 of title 5, United States Code.

(d) LIMITING THE RETENTION OF SENSITIVE PERSONAL DATA.—A covered entity shall delete or de-identify sensitive personal data, and shall direct its service providers to delete or de-identify sensitive personal data, after the data is no longer reasonably necessary to accomplish the intended purposes permitted by this section, unless such deletion or de-identification is impossible or demonstrably impracticable.

(e) BANKRUPTCY.—If a covered entity or service provider commences a case under title 11 of the United States

Code, and the case or any proceeding under the case is expected to lead to the disclosure of the personal data of any individual, the covered entity or service provider shall, in a reasonable amount of time before the disclosure, provide each individual whose personal data is subject to the disclosure with—

(1) a notice of the proposed disclosure, including—

(A) the name of each third party to which the personal data will be disclosed; and

(B) a description of the policies and practices relating to personal data of each such third party; and

(2) the opportunity to—

(A) deny consent, or withdraw previously given consent, to the disclosure of the personal data; or

(B) request that the covered entity or service provider delete or de-identify the personal data.

SEC. 4. RIGHT TO KNOW.

(a) IN GENERAL.—A covered entity shall make publicly available, in a clear and prominent location and in easy-to-understand language, a privacy policy that includes—

(1) a clear and specific description of the entity's policies and practices with respect to personal data;

(2) a clear and specific description of the rights of individuals with respect to their personal data (including the rights described in section 5) and information on how to exercise those rights; and

(3) the information described in subsection (c).

(b) AVAILABILITY OF PREVIOUS VERSIONS.—A covered entity shall make publicly available any previous version of a privacy policy required under subsection (a).

(c) CONTENTS.—A privacy policy required under subsection (a) shall include—

(1) the identity and the contact details of the covered entity, including, where applicable, the representative of the covered entity for purposes of privacy inquiries or its privacy officer;

(2) a clear description of each category of personal data collected by the covered entity and the purposes for which each such category is collected and processed;

(3) a clear description of any relevant retention periods (if possible) and any criteria and other information with respect to the deletion or de-identifica-

tion of personal data collected and processed by the covered entity;

(4) whether, and for what purposes, the covered entity discloses personal data to third parties, each category of personal data disclosed to third parties, and the types of third parties to which those categories of personal data are disclosed;

(5) whether, and for what purposes, the covered entity receives personal data from third parties, the categories of personal data received from third parties, and the types of third parties from which the covered entity receives personal data;

(6) a clear description of the process by which the covered entity informs individuals of material changes to its policies and practices with respect to its collection and processing of personal data;

(7) the specific steps an individual may take to minimize the collection or processing by the covered entity of the individual's personal data, and the relevant implications to the individual from minimizing such collection or processing; and

(8) the effective date of the privacy policy.

(d) EXCEPTIONS.—A covered entity shall not be required to make available a privacy policy under this sub-

section with respect to the collection or processing of personal data that is reasonably necessary and limited to—

(1) an in-person transaction where the personal data is not processed for further purposes incompatible with that transaction;

(2) comply a Federal, State, or local law or another applicable legal requirement, including a subpoena, summons, or other properly executed compulsory process;

(3) prevent imminent danger to the personal safety of any individual; or

(4) protect the rights or data security of the covered entity, a service provider of the covered entity, or any individual, including to investigate a possible crime or to protect against security threats, abuse, fraud, theft, unauthorized transactions, or any other unlawful activity.

(e) MATERIAL CHANGES.—

(1) IN GENERAL.—A covered entity, upon any material change to the privacy policy of the covered entity or a material change to the privacy policy of a service provider that is made at the direction of the covered entity—

(A) shall notify each individual whose personal data is collected or processed by the cov-

ered entity, or a service provider on behalf of the covered entity, with a description of the material change, including—

(i) change to the categories of personal data the covered entity or service provider processes;

(ii) change to the purposes for which the covered entity or service provider processes personal data;

(iii) change to the manner in which the covered entity or service provider discloses personal data to third parties; and

(iv) which, if any, changes are retroactive; and

(B) shall not process (or, in the case of a material change to the privacy policy of a service provider that is directed by the covered entity, shall not direct the service provider to process) any sensitive personal data of an individual that was collected by the covered entity or service provider before the effective date of the material change in a manner that is inconsistent with the privacy policy that was applicable at the time such data was collected until the indi-

vidual provides express affirmative consent to such processing.

(2) DIRECT NOTICE OF MATERIAL CHANGE TO AFFECTED INDIVIDUALS.—A covered entity shall, if operationally and technically feasible, directly provide the notice of a material change required under paragraph (1)(A) to each affected individual, taking into account available technology and the nature of the relationship between the covered entity and the individual.

(3) PUBLIC NOTICE OF MATERIAL CHANGE.—Where directly providing the notice of a material change required under paragraph (1)(A) to each affected individual is impossible or demonstrably impracticable, a covered entity—

(A) shall publish the notice in a reasonably prominent location; and

(B) shall not process personal data that was collected by the covered entity before the effective date of the material change in a manner that is inconsistent with the privacy policy that was applicable at the time such data was collected until after the notice has been so published for a period of time that is reasonably sufficient to give affected individuals the oppor-

tunity to exercise their rights with respect to their personal data.

SEC. 5. INDIVIDUAL CONTROL.

(a) PRIVACY CONTROLS.—Each covered entity shall—

(1) provide each individual whose personal data is collected or processed by the covered entity with a reasonably accessible, clear and conspicuous, and easy-to-use means to exercise the individual's rights established under this section with respect to such data;

(2) if applicable, offer the means required under paragraph (1) through the same means that the individual routinely uses to interact with the covered entity; and

(3) make the means required under paragraph (1) available at no additional cost to the individual.

(b) RIGHT TO ACCESS.—

(1) IN GENERAL.—A covered entity shall, in response to a verified request from an individual—

(A) confirm whether or not the covered entity has collected or processed the personal data of the individual; and

(B) if the covered entity has collected or processed the personal data of the individual,

provide, within a reasonable time after receiving the request, the individual with—

(i) a copy, or an accurate representation, of the personal data pertaining to the individual collected and processed by the covered entity; and

(ii) a list of the categories of third parties to which the covered entity has disclosed the personal data of the individual, if applicable.

(2) EASE OF ACCESS.—

(A) FORMAT.—The covered entity shall provide the information described in paragraph (1)(B) in an electronic format unless—

(i) the individual requests to receive the information by other means; or

(ii) providing the information electronically is impossible or demonstrably impracticable.

(B) DATA PORTABILITY.—If a covered entity provides an individual with information in an electronic format under subparagraph (A), the covered entity shall, where technically feasible and reasonably practicable, provide the individual with—

(i) the ability to export the personal data generated and submitted by the individual in a structured, commonly-used, and machine-readable format; and

(ii) the ability to transmit such information to another entity without constraints or conditions.

(c) RIGHTS TO ACCURACY AND CORRECTION.—

(1) IN GENERAL.—A covered entity shall establish reasonable procedures designed to—

(A) ensure that the personal data that the covered entity collects and processes with respect to an individual is accurate and up-to-date; and

(B) provide individuals with the ability to submit a verified request to the covered entity to—

(i) dispute the accuracy and completeness of such personal data; and

(ii) request the appropriate correction of such personal data.

(2) DISPUTE AND CORRECTION.—Each covered entity shall ensure that the ability of an individual to dispute or request that the covered entity correct personal data as described in paragraph (1) is pro-

vided in a manner that is appropriate and reasonable based on the benefits and risks of harm to the individual regarding the accuracy of the personal data.

(3) EXCEPTIONS FOR PUBLICLY AVAILABLE INFORMATION.—A covered entity shall not be required to verify the accuracy of publicly available information if the covered entity has reasonable procedures to ensure that the publicly available information assembled or maintained by the covered entity accurately reflects the information available to the general public.

(d) RIGHT TO ERASURE.—

(1) IN GENERAL.—Except for personal data collected and processed in accordance with a permissible purpose described in section 3(c), upon a verified request from an individual, a covered entity shall, without undue delay, delete or de-identify the personal data of the individual, and shall direct any service providers of the covered entity to delete or de-identify such data.

(2) SPECIAL CONSIDERATIONS.—In determining whether a covered entity that is a small business has complied with a verified request under paragraph (1) in a timely fashion, the Commission shall take into

account the amount of time that the entity requires to comply with the request considering the technical feasibility, cost, and burden to the entity of complying with the request.

(e) FREQUENCY AND COST TO EXERCISE RIGHTS.—

(1) IN GENERAL.—A covered entity—

(A) shall comply with a verified request from any individual to exercise each of the rights described in subsections (b), (c), and (d) not less frequently than twice in any 12-month period; and

(B) the first 2 times that an individual makes a verified request described in subparagraph (A) in any 12-month period, shall comply with such requests without any charge to the individual.

(2) MANIFESTLY UNFOUNDED AND EXCESSIVE REQUESTS.—If an individual submits a manifestly unfounded or frivolous request to exercise a right under subsection (b), (c), or (d), or an excessive number of requests under such subsections, the covered entity may—

(A) charge a reasonable fee, taking into account the administrative costs of providing the

personal data, communication, or taking the action requested by the individual; or

(B) refuse to act on the request.

(f) VERIFIED REQUEST.—

(1) IN GENERAL.—A request to exercise a right described in this section shall only be considered a ''verified request'' if the covered entity verifies that the individual making the request is the individual whose personal data is the subject of the request.

(2) VERIFICATION OF IDENTITY.—

(A) IN GENERAL.—A covered entity shall make a reasonable effort to verify the identity of any individual who submits a request to exercise a right under this section.

(B) ADDITIONAL INFORMATION.—If a covered entity cannot verify the identity of the individual submitting a request under this subsection, the covered entity—

(i) may request that the individual provide such additional information as is necessary to confirm the identity of the individual; and

(ii) shall only process additional information provided under clause (i) for the

purpose of verifying the identity of the individual.

(g) DECLINATION OF REQUESTS.—

(1) IN GENERAL.—A covered entity—

(A) shall decline to act on a request under this section where, after undertaking a reasonable effort, the entity cannot verify that the individual making the request is the individual whose personal data is the subject of the request;

(B) may decline to act on a request under this section where fulfilling the request would—

(i) require the covered entity or a service provider of the covered entity to retain any personal data collected for a single, one-time transaction, if such personal data is not processed for additional purposes;

(ii) be impossible or demonstrably impracticable, or require any steps or measures to re-identify, or otherwise alter or manipulate, information that is de-identified;

(iii) be contrary to the legitimate interests of the covered entity or a service

provider of the covered entity, such as completing a transaction, repairing functionality or errors, or performing a contract between the covered entity and the individual;

(iv) impair the ability of the covered entity or a service provider of the covered entity to detect or respond to a security incident, provide a secure environment, or protect against malicious, deceptive, fraudulent, or illegal activity;

(v) hinder compliance with a legal obligation or legally recognized privilege, such as a requirement to retain certain information, or the establishment, exercise, or defense of legal claims;

(vi) interfere with research (conducted in accordance with section 3(c)(5)) when the deletion of the personal data is likely to render impossible or seriously impair such research; or

(vii) create a legitimate risk to the privacy, security, safety, or other rights of the individual, an individual other than the requester, or the covered entity, based on

a reasonable individualized determination by the covered entity; and

(C) shall not be required to act on a request under this section if the covered entity is unable to fulfill the request because—

(i) the covered entity requires the assistance of a service provider to fulfill the request; and

(ii) the service provider has informed the covered entity that the service provider is unable to assist the covered entity in fulfilling the request for a reason specified in section 8(c)(3)(A)(ii)(IV).

(2) NOTICE OF REASONS FOR DECLINATION.—If the covered entity declines to act on a request pursuant to paragraph (1), the covered entity shall inform the individual who made the request of the reasons for such declination and any rights the individual may have to appeal the decision of the covered entity.

(h) EXCEPTION FOR SMALL BUSINESSES.—The requirements under subsections (b) and (c) shall not apply to a covered entity that is a small business.

(i) GUIDANCE.—The Commission shall, after consulting with and soliciting comments from consumer data

industry representatives, issue guidance describing non-binding best practices for covered entities and service providers of different business sizes and types to develop privacy controls as described in this section.

SEC. 6. SECURITY.

(a) IN GENERAL.—Each covered entity and service provider shall develop, document, implement, and maintain a comprehensive data security program that contains reasonable administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity of personal data from unauthorized access, use, destruction, acquisition, modification, or disclosure.

(b) CONSIDERATIONS OF SAFEGUARDS.—The safeguards required under subsection (a) with respect to a covered entity or service provider shall be appropriate to—

(1) the size, complexity, and resources of the covered entity or service provider;

(2) the nature and scope of the activities of the covered entity or service provider;

(3) the technical feasibility and cost of available tools, external audits or assessments, and other measures used by the covered entity or service provider to improve security and reduce vulnerabilities;

(4) the sensitivity of the personal data involved; and

(5) the potential for unauthorized access, use, destruction, acquisition, modification, or disclosure of the personal data involved to result in economic loss, identity theft, fraud, or physical injury to the individuals to whom such data relates.

(c) REQUIREMENTS FOR PROGRAM.—A comprehensive data security program under this section shall be designed to, at a minimum—

(1) designate an employee or employees to be responsible for overseeing and maintaining its safeguards;

(2) identify material internal and external risks to the security and confidentiality of personal data and assess the sufficiency of any safeguards in place to control these risks, including consideration of risks in each relevant area of the operations of the covered entity or service provider, including—

(A) employee training and management;

(B) information systems, including network and software design, as well as information processing, storage, transmission, and disposal;

(C) detecting, preventing, and responding to attacks, intrusions, or other systems failures; and

(D) whether the covered entity or service provider has taken action to address and prevent reasonably known and addressable security vulnerabilities;

(3) implement safeguards designed to control the risks identified in the covered entity's or service provider's risk assessment, and regularly assess the effectiveness of those safeguards;

(4) maintain reasonable procedures to require that third parties and service providers to whom personal data is transferred by the covered entity or service provider involved maintain reasonable administrative, technical, and physical safeguards designed to protect the security and confidentiality of personal data; and

(5) evaluate and make reasonable adjustments to the safeguards in light of material changes in technology, internal or external threats to personal data, and the changing business arrangements or operations of the covered entity or service provider.

SEC. 7. ACCOUNTABILITY.

(a) DEFINITION OF APPLICABLE ENTITY.—In this section, the term ''applicable entity'' means a covered entity or service provider that, on an annual basis, conducts collection and processing of—

(1) the personal data of more than 20,000,000 individuals; or

(2) the sensitive personal data of more than 1,000,000 individuals.

(b) PRIVACY OFFICER.—

(1) DESIGNATION.—Each applicable entity shall—

(A) designate an employee of the applicable entity, or an individual who is a contractor of the applicable entity, to be the privacy officer responsible for overseeing its policies and practices relating to the collection and processing of personal data; and

(B) ensure that the privacy officer is involved in all issues relating to the privacy and security of personal data.

(2) CONFLICTS OF INTEREST.—The privacy officer may perform other tasks and duties for the applicable entity, but only to the extent that the applicable entity ensures that the performance of those other tasks or duties does not present a conflict of interest with respect to the duties and responsibilities of the privacy officer role.

(3) RESPONSIBILITIES.—The privacy officer shall—

(A) inform and advise the applicable entity of the obligations of the applicable entity under this Act;

(B) monitor compliance by the applicable entity with this Act;

(C) oversee—

(i) in the case of an applicable entity that is a covered entity, each privacy impact assessment carried out under subsection (c); and

(ii) the comprehensive privacy program implemented under subsection (d); and

(D) act as a contact for the Commission, other Federal, State, and local authorities, and the applicable entity with respect to matters relating to the privacy and security of personal data.

(c) CONSIDERATION OF PRIVACY IMPLICATIONS OF MATERIAL CHANGES IN PROCESSING SENSITIVE PERSONAL DATA.—

(1) IN GENERAL.—If an applicable entity that is a covered entity intends to begin a new collection or processing activity or to make a material change in its processing of sensitive personal data, the ap-

plicable entity shall, before beginning the new processing activity or making the material change, consider the privacy implications, if any of the change.

(2) CONSIDERATIONS.—An applicable entity that is a covered entity shall ensure, in considering the privacy implications of a material change as required under paragraph (1), that the consideration is reasonable and appropriate with respect to the sensitive personal data that will be affected by the new processing activity or the material change in processing by considering—

(A) the nature and volume of the sensitive personal data; and

(B) the potential for the new processing activity or the material change to be a proximate cause of harm to individuals to whom the sensitive personal data pertains.

(3) APPROVAL.—The privacy officer shall be required to approve the findings of a privacy impact assessment carried out under paragraph (1) before a applicable entity that is a covered entity may begin the new processing activity or make the material change that is the subject of the privacy impact assessment.

(4) DOCUMENTATION.—An applicable entity that is a covered entity shall document and maintain in written form any privacy impact assessment carried out under paragraph (1) if the new processing activity or material change that is the subject of the privacy impact assessment involves sensitive personal data.

(d) COMPREHENSIVE PRIVACY PROGRAM.—

(1) IN GENERAL.—Each applicable entity shall implement a comprehensive privacy program to safeguard the privacy and security of personal data collected or processed by the applicable entity for the life cycle of development and operational practices of its products or services, including by—

(A) enhancing the privacy and security of personal data collected or processed by the applicable entity through appropriate technical or operational safeguards, such as encryption, de-identification, and other privacy enhancing technologies;

(B) verifying that the applicable entity's practices relating to the collection and processing of personal data are consistent with—

(i) the entity's policies and documentation of such policies;

(ii) in the case of an applicable entity that is a covered entity, representations the entity makes to individuals; and

(iii) in the case of an applicable entity that is a service provider, representations the entity makes to covered entities to which the entity provides services; and

(C) ensuring that the privacy controls of the applicable entity are adequately accessible to, and effective at safeguarding the expressed preferences of—

(i) in the case of an applicable entity that is a covered entity, each individual whose personal data is collected or processed by the covered entity (excluding any personal data with respect to which the covered entity is a third party); and

(ii) in the case of an applicable entity that is a service provider, each covered entity to which the entity provides services.

(2) CONSIDERATIONS.—In implementing a comprehensive privacy program under paragraph (1), each applicable entity shall—

(A) take into consideration, as applicable given the entity's role as a covered entity or service provider—

(i) the relevant risks to the privacy and security of personal data against which the applicable entity must guard in meeting the expectations of individuals;

(ii) the requirements under this Act;

(iii) the size and complexity of the applicable entity; and

(iv) the sensitivity and volume of the personal data that the applicable entity processes; and

(B) address the findings and implement the recommendations contained in privacy impact assessments that the applicable entity carries out under subsection (c).

SEC. 8. RULES RELATING TO SERVICE PROVIDERS.

(a) OBLIGATIONS OF COVERED ENTITIES WITH RESPECT TO SERVICE PROVIDERS.—

(1) IN GENERAL.—A covered entity shall only disclose personal data to a service provider pursuant to a contract that is binding on both parties and meets the requirements of subsection (b).

(2) DUE DILIGENCE.—

(A) IN GENERAL.—Any covered entity that discloses personal data to a service provider shall—

(i) take reasonable steps to identify whether the service provider has established appropriate procedures and controls for ensuring the privacy and security of the personal data in a manner that complies with the requirements of this Act, including through reasonable representations made to the covered entity by the service provider in the contract governing the disclosure of personal data to the service provider; and

(ii) investigate any circumstances for which a reasonable person would determine that there is a high probability that the service provider is not in compliance with a requirement of this Act, and, if necessary based on the findings of such investigation, take reasonable steps to protect the privacy and security of any personal data disclosed by the covered entity to the service provider that is at risk as a result of the

service provider's noncompliance with a requirement of this Act.

(B) CONSIDERATIONS.—In determining whether a covered entity has acted reasonably in complying with clause (i) or (ii) of subparagraph (A), the Commission shall take into account—

(i) the size, complexity, and resources of the covered entity and whether the covered entity is a small business; and

(ii) the risk of harm reasonably expected to occur as a result of the covered entity disclosing personal data to a service provider without complying with such clause.

(b) CONTRACTUAL REQUIREMENTS.—

(1) IN GENERAL.—A contract between a covered entity and a service provider governing the disclosure of personal data by the covered entity to the service provider shall—

(A) require the service provider to only collect or process the personal data as directed by the covered entity;

(B) establish the purposes for, and means of, the collecting or processing of the personal

data by the service provider, including instructions, policies, and practices, as applicable, with which the service provider is required to comply; and

(C) include a reasonable representation by the service provider indicating that the service provider has established appropriate procedures and controls to comply with the requirements of this Act.

(2) LIMITATION.—No contract governing the disclosure of personal data by a covered entity to a service provider shall relieve a covered entity or service provider of any requirement or obligation with respect to such personal data that is imposed on the covered entity or service provider, as applicable, by this Act.

(c) SERVICE PROVIDER OBLIGATIONS.—

(1) NOTICE OF PROCESSING OF PERSONAL DATA TO COMPLY WITH LEGAL REQUIREMENT.—In the event that a service provider is required to process personal data in order to comply with a legal requirement, including a subpoena, summons, or other properly executed compulsory process, the service provider shall inform the covered entity from which it received the personal data involved of such legal

requirement before such processing, unless the service provider is otherwise prohibited by law from providing such notification.

(2) NOTICE OF CHANGE TO POLICIES OR PRACTICES.—If a service provider amends its policies or practices relating to personal data in a manner that is relevant to compliance with any provision of this Act, the service provider shall provide reasonable notice in advance of such change to any covered entity on whose behalf the service provider collects or processes personal data.

(3) RESPONSIBILITIES.—

(A) INDIVIDUAL CONTROL REQUESTS.—A service provider that collects or processes personal data on behalf of a covered entity shall, to the extent possible, either—

(i) provide the covered entity with appropriate technical and organizational measures to enable the covered entity to comply with requests to exercise rights described in section 5 with respect to any such personal data that is held by, and reasonably accessible to, the service provider; or

(ii) respond to any request made by the covered entity for assistance in complying with a request to exercise such a right with respect to such personal data that the covered entity has verified as described in section 5(f) and has determined must be complied with under this Act by, as appropriate—

(I) in the case of a request described in subsection (b) of section 5, providing the covered entity with access to any relevant personal data held by, and reasonably available to, the service provider;

(II) in the case of a request described in subsection (c) of such section, by correcting any relevant personal data held by, and reasonably accessible to, the service provider, and providing the covered entity with notice of such correction;

(III) in the case of a request described in subsection (d) of such section, by deleting, de-identifying, or returning to the covered entity any rel-

evant personal data held by, and reasonably accessible to, the service provider, and providing the covered entity with notice of such action; or

(IV) informing the covered entity that—

(aa) the service provider does not hold any personal data related to the request;

(bb) the service provider cannot reasonably access any personal data related to the request; or

(cc) complying with the request would be inconsistent with a legal requirement to which the service provider is subject.

(B) DELETION OF DATA UPON COMPLETION OF SERVICE.—Except as otherwise required by law, as soon as practicable after the completion of the service or function for which a service provider collected or processed personal data on behalf of a covered entity, the service provider shall delete, de-identify, or re-

turn to the covered entity all such personal data.

(C) ASSURANCE OF COMPLIANCE.—

(i) IN GENERAL.—Subject to clause (ii), a service provider shall make available to a covered entity on whose behalf the service provider collects or processes personal data information necessary to demonstrate the service provider's compliance with subparagraph (A).

(ii) WRITTEN REPRESENTATION OF COMPLIANCE.—If the information described in clause (i) is not technically available to a service provider, the service provider may comply with clause (i) by providing the covered entity with a written representation stating that the service provider is in compliance with subparagraph (A).

(4) SUBCONTRACTOR REQUIREMENTS.—A service provider that is collecting or processing personal data on behalf of a covered entity shall not employ a subcontractor to carry out or assist in such collection or processing unless—

(A) the service provider has provided the covered entity with an opportunity to object to the use of such subcontractor; and

(B) the subcontractor is subject (pursuant to an agreement between the service provider and the subcontractor) to the same requirements and obligations as the service provider with respect to the collection and processing of the personal data.

(5) CONSIDERATIONS.—In determining whether a service provider has acted reasonably in complying with this subsection, the Commission shall take into account—

(A) the size, complexity, and resources of the service provider and whether the service provider is a small business; and

(B) the risk of harm reasonably expected to occur as a result of the service provider not complying with this subsection.

SEC. 9. ENFORCEMENT.

(a) ENFORCEMENT BY THE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act or a regulation promulgated under this Act shall be treated as an unfair or deceptive act or practice in violation of a rule

promulgated 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 subparagraph (C), the Commission shall enforce this Act and any regulation 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 covered entity or service provider 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.).

(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, with respect to common carriers and nonprofit organizations described in section 2(4) of this Act, in the same manner provided in subparagraphs (A) and (B) of this paragraph.

(D) AUTHORITY PRESERVED.—Nothing in this Act shall be construed to limit the Commission's authority under the Federal Trade Commission Act or any other provision of law.

(3) CIVIL PENALTIES.—

(A) IN GENERAL.—Notwithstanding section 5(m) of the Federal Trade Commission Act (15 U.S.C. 45(m)), in an action brought by the Commission to enforce this Act and the regulations promulgated under this Act, in addition to any injunctive relief obtained by the Commission in the action, a covered entity or service provider shall be liable for a civil penalty in an amount described in subparagraph (B) if the covered entity or service provider, with actual knowledge, violates this Act or a regulation promulgated under this Act.

(B) AMOUNT.—

(i) CALCULATION.—Except as provided in clause (ii), the amount of a civil

penalty described in subparagraph (A) shall be the number of individuals affected by a violation described in that subparagraph multiplied by an amount not to exceed $42,530.

(ii) CONSIDERATIONS.—In determining the amount of a civil penalty to seek under subparagraph (A) for a violation described in that subparagraph, the Commission shall consider, with respect to the covered entity or service provider that committed the violation—

(I) the degree of harm associated with the privacy and security of personal data of individuals created by the violation;

(II) the intent of the covered entity or service provider in committing the violation;

(III) the size, complexity, and resources of the covered entity or service provider, including if it is a small business;

(IV) reasonable expectations relating to privacy and security of personal data of individuals;

(V) the degree to which the covered entity or service provider put in place appropriate controls or complied with the requirements of section 7, if applicable;

(VI) whether the covered entity or service provider self-reported the violation to the Commission; and

(VII) what, if any, efforts the covered entity or service provider has taken to mitigate any risk to the privacy and security of personal data of individuals created by the processing.

(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) CIVIL ACTION.—In any case in which an attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any covered entity or service provider in a practice that violates this Act or a regulation promulgated under this Act, the attorney general of the

State may, as parens patriae, bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to—

(A) enjoin that practice;

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

(C) in the case of a violation described in subsection (a)(3)(A), impose a civil penalty in an amount described in subsection (a)(3)(B).

(2) RIGHTS OF THE COMMISSION.—

(A) NOTICE TO COMMISSION.—

(i) IN GENERAL.—Except as provided in clause (iii), the attorney general of a State shall notify the Commission in writing that the attorney general intends to bring a civil action under paragraph (1) not later than 10 days before initiating the civil action.

(ii) CONTENTS.—The notification required by clause (i) with respect to a civil action shall include a copy of the complaint to be filed to initiate the civil action.

(iii) EXCEPTION.—If it is not feasible for the attorney general of a State to provide the notification required by clause (i)

before initiating a civil action under paragraph (1), the attorney general shall notify the Commission immediately upon instituting the civil action.

(B) INTERVENTION BY THE COMMISSION.—The Commission may—

(i) intervene in any civil action brought by the attorney general of a State under paragraph (1); and

(ii) upon intervening under clause (i)—

(I) be heard on all matters arising in the civil action; and

(II) file petitions for appeal of a decision in the civil action.

(3) CONSOLIDATION OF ACTIONS BROUGHT BY TWO OR MORE STATE ATTORNEYS GENERAL.—

(A) IN GENERAL.—Subject to subparagraph (B), if a civil action under paragraph (1) is pending in a district court of the United States and one or more civil actions are commenced pursuant to paragraph (1) in a different district court of the United States that involve one or more common questions of fact, all such civil actions shall be transferred for the

purposes of consolidated pretrial proceedings and trial to the United States District Court for the District of Columbia.

(B) EXCEPTION.—A civil action shall not be transferred pursuant to subparagraph (A) if pretrial proceedings in such civil action have concluded before the subsequent action is commenced pursuant to paragraph (1).

(c) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission institutes an action under subsection (a) with respect to a violation of this Act or a regulation promulgated under this Act, a State may not, during the pendency of that action, institute an action under subsection (b) against any defendant named in the complaint in the action instituted by the Commission based on the same set of facts giving rise to the violation with respect to which the Commission instituted the action.

(d) NO PRIVATE RIGHT OF ACTION.—There shall be no private right of action under this Act and nothing in this Act may be construed to provide a basis for a private right of action.

SEC. 10. RELATION TO OTHER LAWS.

(a) CONGRESSIONAL INTENT TO PREEMPT STATE PRIVACY AND SECURITY LAW.—It is the express intention

of Congress to promote consistency in consumer expectations, competitive parity, and innovation through the establishment of a uniform Federal privacy framework that preempts, and occupies the field with respect to, the authority of any State or political subdivision of a State over the conduct or activities of covered entities covered by this Act (or under a law enumerated in subsection (c)) relating to the privacy or security of personal data, including consumer controls relating to personal data such as rights to access, correction, and deletion.

(b) EXPRESS PREEMPTION OF STATE LAW.—

(1) IN GENERAL.—Except as provided in paragraph (2), this Act shall supersede any provision of a law, rule, regulation, or other requirement of any State or political subdivision of a State to the extent that such provision relates to the privacy or security of personal data.

(2) PRESERVATION OF STATE AND LOCAL LAWS.—The provisions of this Act shall not be construed to preempt or supersede the applicability of any of the following laws of a State or political subdivision of a State to the extent that such law is not inconsistent with this Act:

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

(B) Rules of criminal or civil procedure.

(C) Laws that relate to the general standards of fraud or public safety.

(D) Laws that address the privacy of any group of students (as defined in section 444(a) of the General Education Provisions Act (20 U.S.C. 1232g(a)) (commonly referred to as the ''Family Educational Rights and Privacy Act of 1974'')).

(E) Laws that address financial information held by financial institutions (as defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809)).

(F) Laws that address protected health information held by covered entities and business associates (as such terms are defined for purposes of regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note)).

(G) Laws governing employment and employment-related data including data collected or used by an employer pursuant to an employer-employee relationship.

(H) Laws protecting the right of individuals to be free of discrimination based on race, sex, national origin, or other suspect classification identified under State law.

(c) RELATION TO OTHER FEDERAL LAWS.—

(1) IN GENERAL.—Except as otherwise provided in paragraphs (2) and (4), this Act shall supersede any other Federal statute or regulation relating to the privacy or security of personal data.

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

(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 Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 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 Electronic Communications Privacy Act (18 U.S.C. 2510 et seq.).

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

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

(3) DEEMED COMPLIANCE.—A covered entity that is required to comply with a law specified in paragraph (2) and is in compliance with the data collection, processing, or security requirements of such law shall be deemed to be in compliance with the requirements of this Act with respect to personal data covered by such law.

(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 supple-

mentary thereto nor any regulation promulgated by the Federal Communications Commission under such Acts shall apply to any covered entity with respect to the collection, use, processing, transferring, or security of personal data, except to the extent that such provision or regulation pertains solely to ''911'' lines or any 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. 11. COMMISSION RESOURCES.

(a) APPOINTMENT OF ATTORNEYS, TECHNOLOGISTS, AND SUPPORT PERSONNEL.—Notwithstanding any other provision of law, the Chair of the Commission shall appoint no fewer than 440 additional individuals to serve as personnel to enforce this Act and other laws relating to privacy and data security that the Commission is authorized to enforce.

(b) ASSESSMENT OF COMMISSION RESOURCES.—Not later than 1 year after the date of enactment of this Act, the Commission shall submit to Congress a report that includes—

(1) an assessment of the resources, including personnel, available to the Commission to carry out this Act; and

(2) a description of any resources, including personnel—

(A) that are not available to the Commission; and

(B) that the Commission requires to effectively carry out this Act.

(c) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Commission such sums as may be necessary to carry out this section.

SEC. 12. GUIDANCE AND REPORTING.

(a) INTERNATIONAL COORDINATION AND COOPERATION.—

(1) IN GENERAL.—If necessary, the Commission shall coordinate any enforcement action by the Commission under this Act with any relevant data protection authority established by a foreign country or any similar office of a foreign country in a manner consistent with subsections (j) and (k) of section 6 of the Federal Trade Commission Act (15 U.S.C. 46).

(2) INTERNATIONAL INTEROPERABILITY.—The Secretary of Commerce, in consultation with the Commission and the heads of other relevant Federal agencies, shall—

(A) identify laws of foreign countries or regions that relate to the processing of personal data for commercial purposes;

(B) engage with relevant officials of foreign countries or regions that have implemented laws described in subparagraph (A) in order to identify requirements under those laws that could disrupt cross-border transfers of personal data;

(C) develop mechanisms and recommendations to prevent disruptions described in subparagraph (B); and

(D) not later than 1 year after the date of enactment of this Act, and once a year each year thereafter for 5 years, submit to Congress a report on the progress of efforts made under this section.

(b) REPORTS TO CONGRESS.—Not later than 180 days after the date of enactment of this Act, and not less frequently than annually thereafter, the Commission shall submit to Congress, and make available on a public website, a report that contains information relating to—

(1) the effectiveness of this Act and regulations promulgated under this Act;

(2) compliance with the provisions of this Act and regulations promulgated under this Act;

(3) violations of the provisions of this Act and regulations promulgated under this Act;

(4) enforcement actions by the Commission and State attorneys general for violations of the provisions of this Act and regulations promulgated under this Act;

(5) priorities of the Commission in enforcing the provisions of this Act and regulations promulgated under this Act; and

(6) resources needed by the Commission to fully implement and enforce the provisions of this Act and regulations promulgated under this Act.

(c) STUDY AND REPORT BY THE GOVERNMENT ACCOUNTABILITY OFFICE.—Not later than 3 years after the date of enactment of this Act, and once every 3 years thereafter, the Comptroller General of the United States shall submit to the President and Congress a report that surveys Federal data privacy and security laws in order to—

(1) identify any inconsistency between the requirements under this Act and the requirements under any law related to the privacy and security of personal data;

(2) review the impact of the provisions of this Act on small businesses and provide recommendations, if necessary, to improve compliance and enforcement;

(3) provide recommendations on amending Federal data privacy and security laws in light of changing technological and economic trends; and

(4) detail the Federal data privacy and security enforcement activities carried out by the Commission and other Federal agencies.

SEC. 13. SEVERABILITY.

If any provision of this Act or the application of such provision to any person or circumstance is held to be unconstitutional, the remainder of this Act, and the application of the provision to any other person or circumstance, shall not be affected.

SEC. 14. EFFECTIVE DATE.

This Act shall take effect on the date that is 1 year after the date of enactment of this Act, except that section 10 shall take effect upon the date of enactment of this Act.

○