.....

(Original Signature of Member)

119TH CONGRESS
2D SESSION

H. R. _____

To establish a national framework for consumer privacy rights and the protection of personal data, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. JOYCE of Pennsylvania introduced the following bill; which was referred to the Committee on _____

A BILL

To establish a national framework for consumer privacy rights and the protection of personal data, and for other purposes.

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

SECTION 1. SHORT TITLE.

(a) SHORT TITLE.—This Act may be cited as the ''Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act'' or the ''SECURE Data Act''.

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

SEC. 2. CONSUMER PRIVACY RIGHTS.

(a) CONSUMER PRIVACY RIGHTS.—A consumer has the following privacy rights with respect to a controller:

(1) To confirm whether a controller is processing the personal data of the consumer and have access to a copy of such data, unless the confirmation and access would require the controller to reveal a trade secret.

(2) To correct any inaccuracy in the personal data of the consumer, taking into account the nature of the personal data and the purpose of processing the personal data.

(3) To delete personal data provided by or obtained about the consumer.

(4) If the data is available in a digital format and to the extent technically feasible, to obtain a copy of the personal data that the consumer previously provided to the controller in a portable and readily usable format that allows the consumer to transmit the data to another controller without hindrance.

(5) To opt out of the processing of the personal data for the following purposes:

(A) Targeted advertising.

(B) The sale of personal data.

(C) Reliance on profiling to make a decision that has a legal or similarly significant effect on the consumer.

(b) CONSENT REQUIRED FOR PROCESSING SENSITIVE DATA.—

(1) IN GENERAL.—Except as provided in paragraphs (2) and (3), a controller may not process the sensitive data of a consumer without obtaining the consent of the consumer before processing.

(2) APPLICABILITY TO A CHILD.—Notwithstanding paragraph (1), a controller shall process the sensitive data of a child in accordance with the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq).

(3) APPLICABILITY TO A TEEN.—Notwithstanding paragraph (1), a controller may not process the sensitive data of a teen without obtaining the verifiable consent of a parent of the teen.

(c) CONSUMER PRIVACY RIGHTS REQUESTS.—

(1) REQUEST FOR CONSUMER RIGHTS.—A controller shall comply with any consumer privacy right described in subsection (a) once a consumer submits a request that specifies each consumer privacy right the consumer requests to exercise and the controller authenticates the consumer.

(2) CHILD AND TEEN CONSUMER RIGHTS.—With respect to a consumer privacy right described in subsection (a) for a child or teen, only a parent of the child or teen may exercise such consumer privacy right on behalf of the child or teen.

(d) CONTROLLER REQUIREMENTS.—

(1) DEADLINE FOR RESPONSE.—Except as provided in paragraph (2), without undue delay and not later than 45 days after the date on which a consumer submits a request under subsection (c), a controller—

(A) shall respond to the consumer and comply with each privacy right requested; or

(B) shall provide a notice to the consumer that—

(i) the controller declines to take action;

(ii) includes a justification for such inaction; and

(iii) includes instructions on how the consumer can appeal the decision of such inaction.

(2) EXTENSION OF RESPONSE PERIOD.—The controller may extend the period described in paragraph (1)(A) an additional 45 days when reasonably necessary, taking into consideration the complexity and number of requests submitted by the consumer, if the controller informs the consumer of the extension during such period with the reason for such extension.

(3) FEES CHARGED.—

(A) FREE OF CHARGE.—For each consumer privacy right described in subsection (a), a consumer may submit to each controller 2 requests under subsection (c) related to such consumer privacy right in a year free of charge.

(B) REASONABLE FEE FOR ADMINISTRATIVE COST.—If a consumer submits more than

2 such requests or submits a request that is technically infeasible or manifestly unfounded, the controller may—

(i) charge the consumer a reasonable fee to cover the administrative costs of complying with the request if the controller has notified the consumer of such fee and the consumer has consented to pay such fee; or

(ii) decline to act on the request.

(C) CONTROLLER DOCUMENTATION REQUIRED.—The controller shall demonstrate, document, and provide to the Commission or a State attorney general, upon request, any technically infeasible or manifestly unfounded nature of any such request.

(4) AUTHENTICATION.—If a controller is unable to authenticate a consumer who submits a request under subsection (c), the controller is not required to comply with such request and may request that the consumer provide additional information reasonably necessary to authenticate the consumer and the request.

(5) PERSONAL DATA OBTAINED FROM THIRD PARTY.—A controller that obtains personal data

about a consumer from a source other than the consumer is considered to be in compliance with the request of a consumer under subsection (c) to delete that personal data under subsection (a)(3) by—

(A) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the personal data of the consumer remains deleted from the records of the controller and not using the retained data for any other purpose under this Act; or

(B) opting the consumer out of the processing of that personal data for any purpose other than a purpose that is exempt under the provisions of this Act.

(6) APPLICABILITY TO A CHILD.—With respect to a request of a consumer under subsection (c) for a child, a controller shall be deemed to be in compliance with such subsection if the controller responds to an equivalent consumer privacy right exercised by a parent under the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq).

(e) APPEAL PROCESS.—

(1) ESTABLISHMENT OF PROCESS.—A controller shall establish a process for a consumer to

appeal a determination by the controller to not take action under subsection (d)(1)(B).

(2) AVAILABILITY.—The appeal process established pursuant to paragraph (1) shall be conspicuously available and similar to the process for a request submitted under subsection (c).

(3) DEADLINE TO RESPOND.—Not later than 60 days after the date on which an appeal is received by a controller, the controller—

(A) shall inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of each reason for a decision; and

(B) if the appeal is denied, shall provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Commission or a State attorney general to submit a complaint.

(f) EXERCISING CONSUMER RIGHTS.—

(1) SUBMISSION OF REQUESTS.—A controller shall establish and describe in a privacy notice one or more secure and reliable means for a consumer to submit a request to exercise consumer privacy rights described under subsection (a).

(2) CONSIDERATIONS.—In establishing the means pursuant to paragraph (1), a controller shall take into account the ways in which a consumer normally interacts with the controller, the need for secure and reliable communication of such requests, and the ability of the controller to authenticate the consumer making the request.

(3) NEW ACCOUNTS NOT REQUIRED.—A controller may not require a consumer to create a new account in order to exercise consumer privacy rights described under subsection (a) but may require a consumer to use an existing account.

SEC. 3. CONTROLLERS.

(a) DATA MINIMIZATION.—A controller shall limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to each purpose for which the data is processed as disclosed to the consumer.

(b) LIMITATION ON SECONDARY USES.—Except as otherwise provided in this section, a controller may not process personal data for any purpose that is not reasonably necessary or compatible with the disclosed purpose for which the personal data is processed as disclosed to the consumer, unless the controller obtains the consent of the consumer before any such processing.

(c) CIVIL RIGHTS.—A controller may not process personal data in violation of a Federal law that prohibits unlawful discrimination against a consumer.

(d) NON-DISCRIMINATION.—A controller may not discriminate against a consumer for exercising any consumer right described under section 2, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods and services to the consumer.

(e) CONSUMER LOYALTY PROGRAMS.—Nothing in subsection (d) may be construed—

(1) to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain; or

(2) to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the offer is related to the voluntary participation of a consumer in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(f) NON-WAIVER OF CONSUMER RIGHTS.—Beginning on the date of the enactment of this Act, any provision of a contract or agreement of any kind that waives or lim-

its a consumer right described under section 2 shall be deemed contrary to public policy and shall be void and unenforceable.

(g) NOTICE TO CONSUMERS.—Before processing the personal data of a consumer, a controller shall provide that consumer with a reasonably accessible, clear, and meaningful privacy notice that includes the following:

(1) Each category of personal data processed by the controller.

(2) Each purpose for processing personal data.

(3) How a consumer may exercise a consumer right described under section 2, including how a consumer may appeal the decision of a controller under section 2(d).

(4) Each category of personal data the controller shares with any other controller or any governmental entity.

(5) Each category of other controllers or any governmental entity, if any, with whom the controller shares personal data.

(6) Whether any personal data processed by the controller is transferred to, processed in, stored in, or sold to a covered nation.

(h) DISCLOSURE OF SALE.—If a controller sells personal data of a consumer, the controller shall clearly and conspicuously disclose—

(1) such activity before any collection or sale of personal data; and

(2) the manner in which a consumer may exercise the right to opt out of the sale of such personal data under section 2(a)(5).

(i) DISCLOSURE OF TARGETED ADVERTISING.—If a controller processes personal data of a consumer for targeted advertising, the controller shall clearly and conspicuously disclose—

(1) such activity before any collection or use of personal data; and

(2) the manner in which a consumer may exercise the right to opt out of such processing under section 2(a)(5).

(j) AUTOMATED DECISION MAKING.—

(1) PROFILING.—A controller that relies on profiling to make a decision that has a legal or similarly significant effect on a consumer shall clearly and conspicuously disclose to such consumer before any such decision is made that—

(A) the decision will be made using automated means; and

(B) the manner in which a consumer may exercise the right to opt out of such profiling.

(2) RELIANCE ON PROFILING.—For purposes of paragraph (1) and section 2(a)(5), a controller relies on profiling to make a decision that has a legal or similarly significant effect on a consumer if such decision is made with no human review, involvement, oversight, or intervention.

SEC. 4. DATA SECURITY.

(a) DATA SECURITY.—A controller shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data and that are appropriate to the volume, sensitivity, and nature of such personal data.

(b) REBUTTABLE PRESUMPTION.—A controller has a rebuttable presumption to an alleged violation of this section if—

(1) the controller complies with a relevant code of conduct approved under section 8(a)(3) (or a relevant certification described in section 8(f)); or

(2) the controller has established, implemented, and maintained—

(A) data security practices appropriate to the state-of-the-art in administrative, technical,

and physical data security practices for the protection of the confidentiality, integrity, and accessibility of personal data, including such a practice demonstrated by adherence to a widely-accepted technical specification or through a third-party attestation; and

(B) a comprehensive data security program that reasonably conforms to a relevant Federal or widely-accepted international risk management framework for identifying and protecting against data security risks, and for detecting, responding to, and recovering from data security events.

SEC. 5. DATA BROKERS.

(a) DISCLOSURE.—A data broker shall post on a publicly available website or mobile application a conspicuous notice that—

(1) states that the entity maintaining the website or application is a data broker;

(2) is clear, not misleading, and readily accessible by the public; and

(3) informs a consumer how to exercise any consumer right described under section 2.

(b) REGISTRATION.—Not later than 12 months after the date of the enactment of this Act, and annually there-

after, a data broker shall register with the Commission by filing a registration statement and paying a reasonable registration fee set by the Commission that includes the following information:

(1) The legal name of the data broker.

(2) A contact person and the primary physical address, e-mail address, telephone number, and website address for the data broker.

(3) A description of each category of personal data sold by the data broker.

(4) A statement of whether the data broker implements a purchaser credentialing process.

(5) A description of any incident of unauthorized access to personal data that the data broker has reported to a Federal or State governmental entity pursuant to an applicable law, rule, or regulation during the year before the year in which the registration is filed, and if known, the total number of consumers affected by each previously reported incident of such unauthorized access.

(6) A link to the privacy policy published in accordance with section 3(g).

(7) A link to a website published by the data broker that informs a consumer how to exercise any consumer right described under section 2.

(c) DATA BROKER REGISTRY.—Not later than 18 months after the date of the enactment of this Act, the Commission shall establish and maintain on a publicly available website of the Commission a searchable, central registry of data brokers registered under subsection (b) that includes the following:

(1) A search feature that allows a person searching the registry to identify a data broker.

(2) For each data broker, a link to the privacy policy published in accordance with section 3(g).

(3) For each data broker, a link to a website published by the data broker that informs a consumer how to exercise any consumer right described under section 2.

SEC. 6. PROCESSORS.

(a) ADHERENCE TO CONTROLLER INSTRUCTIONS.—A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the requirements of this Act, including by taking into account the nature of processing and the information available to the processor—

(1) by appropriate administrative and technical measures, insofar as reasonably practicable, to fulfill the requirements of the controller to respond to an

assertion of any consumer right described under section 2; and

(2) by assisting the controller in meeting the requirements of the controller under section 4.

(b) CONTRACTUAL OBLIGATION.—A contract between a controller and a processor shall govern the data processing procedures of the processor with respect to processing performed on behalf of the controller. The contract shall clearly set forth instructions for processing personal data, the nature and purpose of processing, the type of personal data subject to processing, the duration of processing, and the rights and obligations of both parties.

(c) MINIMUM REQUIREMENTS.—At a minimum, the contract between a controller and processor shall include requirements that the processor does the following:

(1) Ensures that each person processing personal data is subject to a duty of confidentiality with respect to the data.

(2) At the direction of the controller, deletes or returns all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law.

(3) Upon the reasonable request of the controller, makes available to the controller all informa-

tion in the possession of the processor necessary to demonstrate compliance by the processor with the requirements of this Act.

(4) Either—

(A) allows and cooperates with reasonable assessments by the controller or a designated assessor by the controller; or

(B) the processor—

(i) arranges for a qualified and independent assessor to conduct an assessment of the policies and administrative and technical measures of such processor that meet the requirements of this Act using an appropriate and accepted control standard or framework and assessment procedure for such assessment; and

(ii) provides a report of the assessment to the controller upon request.

(5) If a processor engages a subcontractor, include in any subcontract a requirement that the subcontractor meet the obligations of the processor with respect to the personal data.

(d) RULE OF CONSTRUCTION.—Nothing in this section may be construed to relieve a controller or processor

from any liability imposed on the controller or processor by virtue of a role in a processing.

(e) APPLICABILITY.—

(1) CONTROLLER OR PROCESSOR.—The determination about whether a person is acting as a controller or processor with respect to a specific processing of personal data is a fact-based determination that depends upon the context in which personal data is to be processed.

(2) CONTROLLER.—If a processor, alone or jointly with others, begins determining the purpose and means of processing personal data, such processor is a controller with respect to a specific processing of such personal data.

(3) PROCESSOR.—A processor that follows the instructions of a controller with respect to a specific processing of personal data remains a processor.

SEC. 7. DEIDENTIFIED AND PSEUDONYMOUS DATA.

(a) IN GENERAL.—A controller in possession of deidentified data shall—

(1) take reasonable measures to ensure the data cannot be associated with an individual;

(2) publicly commit to maintain and use deidentified data without attempting to re-identify the data; and

(3) contractually obligate any recipient of the deidentified data to comply with each requirement of this Act.

(b) ONGOING COMPLIANCE.—A controller that discloses deidentified or pseudonymous data shall exercise reasonable oversight to monitor compliance with any contractual commitment to which the deidentified or pseudonymous data is subject and shall take appropriate steps to address any breach of such contractual commitment.

(c) PSEUDONYMOUS DATA.—An assertion of any consumer right described under section 2 does not apply to pseudonymous data for a case in which the controller is able to demonstrate any information necessary to identify the consumer is kept separately and is subject to appropriate administrative and technical measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

(d) RULE OF CONSTRUCTION RELATING TO DEIDENTIFIED OR PSEUDONYMOUS DATA.—Nothing in this Act may be construed to require a controller or processor to—

(1) re-identify deidentified data or pseudonymous data; or

(2) maintain data in identifiable form, or collect, obtain, retain, or access any data or technology,

in order to be capable of associating a consumer request with personal data.

(e) RULE OF CONSTRUCTION RELATING TO CONSUMER RIGHTS REQUESTS.—Nothing in this Act may be construed to require a controller or processor to comply with an assertion of any consumer right described under section 2 if—

(1) the controller is not reasonably capable of associating the request with the personal data or it would be unduly burdensome for the controller to associate the request with the personal data;

(2) the controller does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data, or associate the personal data with other personal data about the same specific consumer; and

(3) the controller does not sell the personal data to another controller or otherwise voluntarily disclose the personal data to any entity other than a processor, except as otherwise permitted in this section.

SEC. 8. CODES OF CONDUCT.

(a) APPLICATION FOR APPROVAL OF CODE OF CONDUCT.—

(1) IN GENERAL.—A controller or processor (or a group of controllers or processors) may submit to the Secretary an application for approval of a code of conduct that meets or exceeds the requirements of the controller or processor (or the group of controllers or processors) under this Act.

(2) APPLICATION REQUIREMENTS.—An application submitted under paragraph (1) shall include the following:

(A) A description of the specific requirements of this Act to which the code of conduct proposed in the application will apply.

(B) A description of how the code of conduct will meet or exceed such requirements.

(C) A description of the entities the code of conduct is designed to cover.

(D) A list of the controllers or processors, to the extent known at the time of application, that intend to comply with the code of conduct.

(E) A description of the independent organization that will administer the code of conduct with respect to controllers or processors, including an explanation of how the independent organization is governed.

(F) A description of how the entities described in subparagraph (C) will be assessed for compliance with the code of conduct by the independent organization described in subparagraph (E).

(G) A description of how the independent organization will refer to the Commission or to a State attorney general any controller or processor that does not—

(i) meet the requirements of this Act; or

(ii) meet or exceed the requirements of the Act in accordance with the certification publicly disclosed by the controller or processor under subsection (c).

(3) REVIEW BY SECRETARY.—

(A) INITIAL APPROVAL.—

(i) PUBLIC COMMENT PERIOD.—Not later than 90 days after the date on which the Secretary receives an application submitted under paragraph (1), the Secretary shall publish the application and provide an opportunity for public comment on the code of conduct proposed in the application.

(ii) APPROVAL CRITERIA.—The Secretary, in consultation with the Commission, shall approve an application submitted under paragraph (1), including the independent organization that will administer the code of conduct, if the controller or processor (or the group of controllers or processors) that submits the application demonstrates that the code of conduct proposed in the application meets the following criteria:

(I) Meets or exceeds the relevant requirements of this Act.

(II) Provides for regular review and validation by the independent organization to ensure that the controller or processor (or the group of controllers or processors) that complies with the code of conduct continues to meet or exceed the relevant requirements of this Act.

(III) Includes referral to the Commission for enforcement or referral to the appropriate State attorney general for enforcement.

(iii) TIMELINE.—Not later than 1 year after the date on which the Secretary receives an application submitted under paragraph (1), the Secretary shall issue a public determination approving or denying the application and providing the reasons for such approval or denial.

(B) APPROVAL OF MODIFICATIONS.—

(i) IN GENERAL.—If an independent organization that administers a code of conduct approved under subparagraph (A) makes significant updates to the code of conduct—

(I) the independent organization shall submit to the Secretary an application for approval of the significant updates made to the code of conduct; and

(II) not later than 90 days after the date on which the Secretary receives an application for an updated code of conduct submitted under subclause (I), the Secretary shall publish the proposed updated code of conduct

and provide an opportunity for public comment.

(ii) TIMELINE.—Not later than 180 days after the date on which the Secretary receives an application for an updated code of conduct submitted under clause (i)(I), the Secretary, considering the approval criteria described in subparagraph (A)(ii), shall issue a public determination approving or denying the application and providing the reasons for such approval or denial.

(b) WITHDRAWAL OF APPROVAL.—

(1) IN GENERAL.—If the Secretary has clear and convincing evidence that a code of conduct approved under subsection (a)(3) no longer meets the relevant requirements of this Act or that compliance with the code of conduct is insufficiently assessed by the independent organization that administers the code of conduct, the Secretary shall notify the relevant controller or processor (or the relevant group of controllers or processors) and the independent organization of a potential withdrawal of approval by the Secretary and of the opportunity to cure any alleged deficiency under paragraph (2).

(2) OPPORTUNITY TO CURE.—

(A) IN GENERAL.—Not later than 180 days after the date on which a controller or processor (or a group of controllers or processors) receives the notice described in paragraph (1), the controller or processor (or the group of controllers or processors) and the relevant independent organization may—

(i) create a proposed cure to any alleged deficiency of the code of conduct or the enforcement of the code of conduct; and

(ii) submit each such proposed cure to the Secretary.

(B) REVIEW OF PROPOSED CURE.—If the Secretary determines within 60 days that a proposed cure submitted under subparagraph (A)(ii) eliminates an alleged deficiency of the code of conduct or the assessment of compliance with the code of conduct, the Secretary may not withdraw the approval of such code of conduct on the basis of such deficiency.

(3) WITHDRAWAL OF APPROVAL.—

(A) DETERMINATION.—If the Secretary determines that a proposed cure submitted

under subparagraph (A)(ii) does not eliminate an alleged deficiency of the code of conduct or the assessment of compliance with the code of the conduct, the Secretary may withdraw approval of such code of conduct on the basis of such deficiency.

(B) NOTIFICATION.—Not later than 10 days after the date on which the Secretary makes a determination under subparagraph (A), the Secretary shall notify the relevant controller or processor (or the relevant group of controllers or processors) and the independent organization of the relevant withdrawal of approval described in subparagraph (A).

(C) EFFECT.—A withdrawal of approval described in subparagraph (A) shall take effect on the date that is 30 days after the date on which the Secretary provides the notification required by subparagraph (B).

(D) PUBLICATION.—Not later than 30 days after the date on which the Secretary provides notification required by subparagraph (B, the Secretary shall publish on a publicly available website a notice about the relevant with-

drawal of approval described in subparagraph (A).

(c) PUBLIC DISCLOSURE.—A controller or processor that participates in a code of conduct approved under subsection (a)(3) shall certify on a publicly available website that the controller or processor is in compliance with the code of conduct, including by listing the independent organization that administers the code of conduct.

(d) REBUTTABLE PRESUMPTION.—A controller or processor that complies with a relevant code of conduct approved under subsection (a)(3) (or a relevant certification described in subsection (f)) shall be entitled to a rebuttable presumption that the controller or processor is in compliance with the relevant requirements of this Act to which the code of conduct (or certification) applies.

(e) CODES OF CONDUCT FOR SMALL BUSINESSES.—

(1) IN GENERAL.—Not later than 2 years after the date of the enactment of this Act, the Secretary shall publish codes of conduct for businesses that otherwise would be persons to whom this Act applies but that do not meet the applicability requirements described in section 13(a)(2).

(2) PROCEDURES.—In carrying out paragraph (1), the Secretary shall—

(A) follow the same procedures described in subsections (a) and (b); and

(B) solicit independent organizations to administer the codes of conduct.

(3) REQUIREMENTS FOR CODE OF CONDUCT.—A code of conduct published under paragraph (1) shall meet the following requirements:

(A) Be consistent with the requirements of this Act.

(B) Be cost-effective for any participant in the code of conduct.

(C) Be appropriate to the risks, size, and limitations of any such participant.

(4) VOLUNTARY PARTICIPATION.—Participation in a code of conduct published under paragraph (1) shall be voluntary.

(5) REQUIREMENTS FOR PARTICIPATION.—A participant in a code of conduct published under paragraph (1) shall publicly self-certify that the participant is in compliance with the code of conduct, including by listing the independent organization that administers the code of conduct.

(f) CROSS-BORDER PRIVACY RULES SYSTEM.—A certification by a controller pursuant to the Global Cross Border Privacy Rules System, or any successor system,

or a certification by a processor pursuant to the Global Cross Border Privacy Rules System Privacy Recognition for Processors, or any successor system, shall be treated as participation in a code of conduct approved under subsection (a)(3).

SEC. 9. CROSS-BORDER DATA FLOWS.

(a) PRINCIPAL ADVISOR.—The Secretary shall serve as the principal advisor to the President on policy relating to the international flow of personal data and the protection of personal data in international commerce.

(b) DUTIES.—The Secretary shall take any action necessary and appropriate to support the international flow of personal data and the protection of personal data in international commerce, including the following:

(1) Assessing the laws, regulations, requirements, frameworks, and practices (and the implementation thereof) of foreign governments for—

(A) alignment with the consumer rights and protections of personal data described in this Act;

(B) any impact on consumers and businesses in the United States, including with respect to economic competitiveness, innovation, and data security; and

(C) any impact on the economic and security interests of the United States.

(2) Developing policy and recommendations relating to—

(A) identifying the benefits of the international flow of personal data to consumers and businesses, including economic competitiveness, innovation, and data security;

(B) addressing any negative impact on consumers and businesses in the United States of laws, regulations, requirements, frameworks, and practices (and the implementation thereof) of foreign governments that limit or restrict the international flow of personal data;

(C) promoting the protection of personal data in a manner that maintains the international flow of personal data in international commerce; and

(D) mitigating the risk posed by covered nations to the international flow of personal data and the protection of personal data in international commerce.

(3) Establishing, maintaining, and promoting frameworks, certifications, principles, and partnerships to facilitate the international flow of personal

data for commercial purposes and the protection of personal data in international commerce.

(4) Coordinating with any relevant agency as needed.

(c) INTERNATIONAL COOPERATION.—

(1) AUTHORITY TO ENTER AGREEMENT.—The Secretary, as the Secretary determines appropriate, may enter into an agreement with a foreign government, international forum, or foreign political or economic union to promote the international flow of personal data and the protection of personal data in international commerce.

(2) REQUIREMENTS FOR AGREEMENT.—Any agreement entered into pursuant to paragraph (1)—

(A) may not have provisions that conflict with the protections for personal data described in this Act;

(B) shall be consistent with the economic and security interests of the United States; and

(C) not later than 60 days after the date on which the agreement is entered into, shall be submitted to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

(d) RULE OF CONSTRUCTION.—Nothing in this section may be construed to alter the authority of any agency with rulemaking and enforcement authority under subtitle A of title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).

SEC. 10. STUDY ON UNIVERSAL OPT-OUT MECHANISMS.

(a) STUDY.—Not later than 3 years after the date of the enactment of this Act, the Secretary shall publish on a publicly available website a report that—

(1) is developed through a process of public consultation;

(2) reviews commercially available technologies, including a web browser setting or extension or a global setting on an electronic device, that allow a consumer to opt out of the processing of the personal data of the consumer by a controller;

(3) considers the feasibility of a universal opt-out mechanism in a manner that makes use of commercially available technologies and accounts for beneficial uses of personal data; and

(4) limits such review and consideration in accordance with the scope of this Act.

(b) COMMERCIALLY AVAILABLE TECHNOLOGIES.—The commercially available technologies reviewed pursuant

to the study required by subsection (a) shall meet the following requirements:

(1) Shall require a consumer to make an affirmative, freely given, and unambiguous choice to indicate the intent of the consumer to opt out of any processing of the personal data of the consumer by a controller.

(2) Shall be consumer-friendly and easy to use by the average consumer.

(3) May not unduly burden lawful data processing by a controller or processor, including with respect to beneficial uses of personal data.

SEC. 11. RULES OF CONSTRUCTION.

(a) IN GENERAL.—Nothing in this Act may be construed to restrict the ability of a controller or processor to do any of the following:

(1) Cooperate with a law enforcement agency with respect to conduct or activity that the controller or processor reasonably and in good faith believes may violate a Federal, State, or local law, rule, or regulation.

(2) Investigate, establish, exercise, prepare for, or defend a legal claim.

(3) Provide a product or service specifically requested by a consumer or a parent of a consumer (if the consumer is a child or teen).

(4) Perform a contract to which a consumer or a parent of a consumer (if the consumer is a child or teen) is a party, including by fulfilling the terms of a written warranty.

(5) Take immediate steps to protect an interest that is essential to the life or physical safety of a consumer or of another individual.

(6) Prevent, detect, protect against, or respond to a security incident, including a data security incident, identity theft, fraud, harassment, malicious or deceptive activity, or any other similar illegal activity.

(7) Preserve the integrity or security of systems.

(8) Investigate, report, or prosecute a person responsible for any such security incident.

(9) Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to any applicable Federal or State ethics or privacy law and is approved, monitored, and governed by an institutional review board (or similar

independent oversight entity) that considers the following:

(A) If the deletion of the personal data of a consumer is likely to provide substantial benefits that do not exclusively accrue to the controller.

(B) If the controller has implemented reasonable safeguards to mitigate privacy and data security risks to a consumer associated with research, including any risks associated with re-identification of the personal data of the consumer.

(C) If the expected benefits of the research outweigh such privacy and data security risks.

(b) PERSONAL DATA.—Nothing in this Act may be construed to restrict the ability of a controller or processor to collect, use, or retain the personal data of a consumer to do any of the following:

(1) Conduct internal research to develop, improve, or repair a product, service, or technology.

(2) Effectuate a product recall.

(3) Identify and repair any technical error that impairs the functionality of a product, service, or technology.

(4) Perform an internal operation that—

(A) is reasonably aligned with the expectations of a consumer;

(B) is reasonably anticipated based on the relationship of a consumer with the controller; or

(C) is otherwise compatible with processing data to—

(i) provide a product or service specifically requested by a consumer or a parent of a consumer (if the consumer is a child or teen); or

(ii) perform a contract to which a consumer or a parent of a consumer (if the consumer is a child or teen) is a party.

(c) PRIVILEGED COMMUNICATION.—Nothing in this Act may be construed to prevent a controller or processor from providing the personal data of a consumer to a person covered by an evidentiary privilege under Federal or State law as part of a privileged communication.

(d) PROTECTED DISCLOSURE.—A controller or processor that discloses the personal data of a consumer to another controller or processor in compliance with the requirements of this Act does not violate this Act if the controller or processor that receives and processes such personal data violates this Act if, at the time of disclosing

the personal data, the disclosing controller or processor did not have knowledge that the receiving controller or processor intended to commit such a violation.

(e) PROTECTED RIGHTS.—Nothing in this Act may be construed as a requirement imposed on a controller or processor that adversely affects the privacy or any other right or freedom of any person, including the right to freedom of speech under the Constitution of the United States, or that applies to the processing of personal data by a person in the course of a purely personal or household activity.

SEC. 12. ENFORCEMENT.

(a) ENFORCEMENT BY COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act shall be treated as a violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—Except as provided in paragraphs (3) and (4), the Commission shall enforce 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, and any person who violates this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

(3) COMMON CARRIERS.—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 Federal Trade Commission, the Federal Trade Commission shall also enforce this Act, in the same manner provided in paragraphs (1) and (2), with respect to common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.).

(4) CIVIL RIGHTS VIOLATIONS.—

(A) EXCEPTION.—Notwithstanding paragraphs (1), (2), and (3), the Commission may not enforce any violation of section 3(c) of this Act.

(B) TRANSMISSION BY COMMISSION.—If the Commission receives information alleging that a controller is in violation of section 3(c), the Commission shall transmit such information, as allowable under Federal law, to any agency with authority to initiate an enforce-

ment action or proceeding relating to the alleged violation described in the information.

(b) ACTIONS BY STATES.—

(1) IN GENERAL.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of such State has been or is threatened or adversely affected by an act or practice in violation of this Act, the attorney general, 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—

(A) enjoin such act or practice;

(B) enforce compliance with this Act;

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

(D) obtain such other legal and equitable relief as the court may consider to be appropriate.

(2) NOTICE.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Commission a written notice of such action and a copy of the complaint for such action. If the attorney general determines that it is not feasible to provide the notice described in this para-

graph before the filing of the action, the attorney general shall provide written notice of the action and a copy of the complaint to the Commission immediately upon the filing of the action.

(3) AUTHORITY OF COMMISSION.—

(A) IN GENERAL.—On receiving notice under paragraph (2) of an action under this subsection, the Commission shall have the right—

(i) to intervene in the action;

(ii) upon so intervening, to be heard on all matters arising therein; and

(iii) to file petitions for appeal.

(B) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission or the Attorney General of the United States has instituted a civil action for violation of this Act (referred to in this subparagraph as the ''Federal action''), no State attorney general may bring an action under this subsection during the pendency of the Federal action against any defendant named in the complaint in the Federal action for any violation of this Act alleged in such complaint.

(4) RULE OF CONSTRUCTION.—For purposes of bringing a civil action under this subsection, nothing in this Act may be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of such State to conduct investigations, administer oaths and affirmations, or compel the attendance of witnesses or the production of documentary and other evidence.

(c) RIGHT TO CURE.—

(1) IN GENERAL.—Neither the Commission nor a State attorney general may initiate any action for a violation of this Act until—

(A) the Commission or the attorney general has provided written notice to a controller or processor alleged to be in violation of this Act of the alleged violation that identifies the specific provision of this Act alleged to have been violated; and

(B) not fewer than 45 days have passed since the date on which such written notice has been provided.

(2) EFFECT OF CURE.—There shall be no violation of this Act with respect to an allegation made under paragraph (1)(A) if, during the period of time

described in paragraph (1)(B), the controller or processor alleged to be in violation of this Act cures the alleged violation of this Act and provides the Commission or the State attorney general with a written statement that such violation has been cured and that no such further violation shall occur.

(3) FAILURE TO CURE.—The Commission or the State attorney general may initiate an action pursuant to subsection (a) or (b) (as the case may be) to remedy an allegation made under paragraph (1)(A) if the controller or processor alleged to be in violation of this Act—

(A) fails to cure the alleged violation pursuant to paragraph (2); or

(B) after curing the alleged violation pursuant to paragraph (2), continues to violate this Act.

SEC. 13. APPLICABILITY.

(a) IN GENERAL.—This Act shall apply to any person that is subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.) or is a common carrier subject to title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.) and—

(1) with respect to the business of the person—

(A) conducts business in the United States or offers for use or sale to a resident of the United States a product or service; or

(B) processes or engages in the sale of personal data of a resident of the United States; and

(2) with respect to personal data and annual gross revenue in the course of such business—

(A) collects and processes personal data of more than 200,000 consumers annually (excluding personal data controlled or processed solely for the purpose of completing a payment transaction) and has an annual gross revenue of $25,000,000 or more (as adjusted on January 1 each year by the percentage increase (if any), during the preceding 12-month period, in the Consumer Price Index for All Urban Consumers published by the Bureau of Labor Statistics); or

(B) collects and processes personal data of 100,000 or more consumers annually (excluding personal data controlled or processed solely for the purpose of completing a payment transaction) and derives 25 percent or more of the

annual gross revenue of the person from the sale of such personal data.

(b) EXEMPTIONS.—This Act does not apply to the following:

(1) A Federal, State, or local governmental entity.

(2) An entity that collects, processes, retains, or transfers personal data on behalf of such Federal or State governmental entity, to the extent that such entity is acting as a processor to the governmental entity.

(3) A financial institution subject to title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).

(4) A covered entity or business associate subject to parts 160 and 164 of title 45, Code of Federal Regulations.

(5) A nonprofit organization.

(6) A nonprofit organization with the primary mission of preventing, investigating, or deterring fraud, training anti-fraud professionals, or educating the public about fraud, including insurance fraud, securities fraud, and financial fraud.

(7) An institution of higher education.

(8) The National Center for Missing and Exploited Children.

(9) An entity created by a Federal or State statute to pay for claims arising from the liquidation of an insurance company.

(10) A futures association registered pursuant to section 17 of the Commodity Exchange Act (7 U.S.C. 21).

(11) A national securities association registered pursuant to section 15A of the Securities Exchange Act of 1934 (15 U.S.C. 78o–3).

(12) Data processed or maintained—

(A) by an individual applying to, employed by, or acting as an agent or independent contractor of a controller or processor for such application, employment, or action;

(B) for inclusion in the emergency contact information relating an individual; or

(C) that is necessary for the administration of benefits for an individual.

(13) The following information:

(A) Health information protected under and collected or used for public health activities and purposes in accordance with HIPAA.

(B) Health records.

(C) Records relating to the identity, diagnosis, prognosis, or treatment of a patient under section 543 of the Public Health Service Act (42 U.S.C. 290dd–2).

(D) Data, information, or identifiable private information (as such term is defined in section 46.102 of title 45, Code of Federal Regulations) obtained pursuant to any of the following:

(i) Part 46 of title 45, Code of Federal Regulations.

(ii) The Guideline for Good Clinical Practice E6(R3) issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use.

(iii) Part 50 or part 56 of title 21, Code of Federal Regulations.

(E) Information reported pursuant to the Health Care Quality Improvement Act of 1986 (42 U.S.C. 11101 et seq.).

(F) Identifiable patient safety work product and nonidentifiable patient safety work product (as such terms are defined in section 921 of the Public Health Service Act (42

U.S.C. 299b–21)) protected under Part C of title IX of the Public Health Service Act (42 U.S.C. 299b–21 et seq.).

(G) Information derived from any of the health care related information listed in this paragraph that is de-identified in accordance with section 164.514(e) of title 45, Code of Federal Regulations.

(H) Information that is included in a limited data set in accordance with the standards and specifications under section 164.514(e) of title 45, Code of Federal Regulations.

(I) Personal data that—

(i) may impact the creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living of a consumer; and

(ii) is collected or disclosed by a consumer reporting agency (as such term is defined in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f))) or a furnisher, to the extent that the consumer reporting agency or furnisher is engaged in activities subject to the Fair Credit Reporting Act.

(J) Personal information (as such term is defined in section 2725 of title 18, United States Code) collected, processed, sold, or disclosed under section 2721 of title 18, United States Code.

(K) Personally identifiable information and personally identifiable data regulated in accordance with section 444 of the General Education Provisions Act (commonly known as the ''Family Educational Rights and Privacy Act of 1974'') (20 U.S.C. 1232g).

(L) Personal data collected, processed, sold, or disclosed as a result of an activity authorized under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.).

(M) Nonpublic personal information (as such term is defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809)).

(N) Any information that originates from, is intermingled with, or is treated in the same manner as information described in subparagraphs (A) through (M) that is maintained by the following:

(i) A covered entity or business associate.

(ii) A program or a qualified service organization (as such terms are defined in section 2.11 of title 42, Code of Federal Regulations).

SEC. 14. RELATIONSHIP TO FEDERAL LAWS.

(a) IN GENERAL.—Nothing in this Act may be construed to relieve or change an obligation that a controller or processor may have under any of the following:

(1) The Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq).

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

(3) Part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.).

(4) Subtitle D of the HITECH Act (42 U.S.C. 17921 et seq.).

(5) Any regulations promulgated under section 264(c) of HIPAA (42 U.S.C. 1320d–2 note).

(6) The requirements regarding the confidentiality of substance use disorder information under section 543 of the Public Health Service Act (42 U.S.C. 290dd–2) or any regulation promulgated under such section.

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

(8) Section 444 of the General Education Provisions Act (commonly known as the ''Family Educational Rights and Privacy Act of 1974'') (20 U.S.C. 1232g) and part 99 of title 34, Code of Federal Regulations (or any successor regulation), to the extent a controller or processor is an educational agency or institution (as such term is defined in 99.3 of such title (or any successor regulation)).

(9) The regulations related to the protection of human subjects under part 46 of title 45, Code of Federal Regulations.

(10) The Health Care Quality Improvement Act of 1986 (42 U.S.C. 11101 et seq.).

(11) Part C of title IX of the Public Health Service Act (42 U.S.C. 299b–21 et seq.).

(12) Chapter 123 of title 18, United States Code.

(b) RELATIONSHIP TO COMMUNICATIONS ACT OF 1934.—

(1) IN GENERAL.—Except as provided in paragraph (2), the Communications Act of 1934 (47 U.S.C. 151 et seq.), and any regulation promulgated by the Federal Communications Commission pursuant to such Act, shall not apply to a controller or

processor with respect to the collection, use, processing, transferring, or security of personal data.

(2) EXCEPTION.—Paragraph (1) does not apply to the extent a regulation or order pertains solely to emergency services.

(c) REPEAL.—Section 2710 of title 18, United States Code, is repealed.

SEC. 15. RELATIONSHIP TO STATE LAWS.

No State or political subdivision of a State may prescribe, maintain, or enforce any law, rule, regulation, requirement, standard, or other provision having the force and effect of law, if such law, rule, regulation, requirement, standard, or other provision relates to the provisions of this Act.

SEC. 16. DEFINITIONS.

In this Act:

(1) AFFILIATE.—

(A) IN GENERAL.—The term ''affiliate'' means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity.

(B) CONTROL; CONTROLLED.—In subparagraph (A), the terms ''control'' and ''controlled'' mean—

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

(ii) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(iii) the power to exercise controlling influence over the management of a company.

(2) AGENCY.—The term ''agency'' has the meaning given that term in section 551 of title 5, United States Code.

(3) AUTHENTICATE.—The term ''authenticate'' means to verify through commercially reasonable means that the consumer, entitled to exercise the consumer rights described under section 2, is the same consumer that exercises such a consumer right with respect to the relevant personal data.

(4) BIOMETRIC DATA.—The term ''biometric data''—

(A) means data generated by automatic measurements of the biological characteristics of an individual, such as a fingerprint, voiceprint, eye retinas, irises, or other unique

biological patterns or characteristics that is used to identify a specific individual; and

(B) does not include a physical or digital photograph, a video or audio recording (or data generated therefrom), or information collected, used, or stored for health care treatment, payment, or operations pursuant to HIPAA.

(5) BUSINESS ASSOCIATE; COVERED ENTITY; HEALTHCARE PROVIDER; PROTECTED HEALTH INFORMATION.—The terms ''business associate'', ''covered entity'', ''healthcare provider'', and ''protected health information'' have the meanings given those terms in for purposes of regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act (42 U.S.C. 1320d–2 note).

(6) CHILD.—The term ''child'' means an individual who is under the age of 13.

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

(8) CONSENT.—The term ''consent''—

(A) means a clear affirmative act that signifies the freely given, specific, informed, and unambiguous agreement by a consumer to process personal data relating to the consumer; and

(B) includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

(9) CONSUMER.—The term ''consumer'' means—

(A) an individual that acts in an individual or household capacity; and

(B) does not include an individual that acts in a commercial or employment context.

(10) CONTROLLER.—The term ''controller'' means a person that, alone or jointly with others, determines the purpose and means of processing personal data.

(11) COVERED NATION.—The term ''covered nation'' has the meaning given that term in section 4872(f) of title 10, United States Code.

(12) DATA BROKER.—

(A) IN GENERAL.—The term ''data broker'' means a controller that meets the following—

(i) The controller collects and processes personal data concerning a consumer who is not:

(I) a customer or a client of the controller; or

(II) a user, reader, or subscriber of a product or service provided by the controller; and

(ii) The controller derives 50 percent or more of annual gross revenue from the sale of such personal data.

(B) LIMITATION.—The term ''data broker'' does not include a person acting as a processor.

(13) DECISION THAT HAS A LEGAL OR SIMILARLY SIGNIFICANT EFFECT.—The term ''decision that has a legal or similarly significant effect'' means a decision made by a controller about a consumer to deny one of the following to the consumer:

(A) A healthcare service (as defined in part 318.2 of title 16, Code of Federal Regulations).

(B) A rental or lease of housing.

(C) An employment opportunity.

(14) DEIDENTIFIED DATA.—The term ''deidentified data'' means data that cannot reasonably be linked to an identified or identifiable individual or a device linked to an individual.

(15) HEALTH RECORD.—The term ''health record'' means a record, other than for financial or

billing purposes, relating to an individual, kept by a health care provider as a result of the professional relationship established between the health care provider and the individual.

(16) HIPAA.—The term ''HIPAA'' means Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d et seq.).

(17) IDENTIFIED OR IDENTIFIABLE NATURAL PERSON.—The term ''identified or identifiable natural person'' means a person who can be readily identified, directly or indirectly.

(18) INSTITUTION OF HIGHER EDUCATION.—The term ''institution of higher education'' has the meaning given that term in section 101 of Higher Education Act of 1965 (20 U.S.C. 1001).

(19) NONPROFIT ORGANIZATION.—The term ''nonprofit organization'' means an organization that is described in section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from taxation under section 501(a) of such Code.

(20) PARENT.—The term ''parent'', with respect to a child or teen, means an adult with the legal right to make decisions on behalf of the child or teen, including—

(A) a natural parent;

(B) an adoptive parent;

(C) a legal guardian; and

(D) an individual with legal custody over the child or teen.

(21) PERSONAL DATA.—The term ''personal data''—

(A) means any information that is linked or reasonably linkable to an identified or identifiable natural person; and

(B) does not include deidentified data or publicly available information.

(22) PRECISE GEOLOCATION DATA.—The term ''precise geolocation data''—

(A) means information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with precision and accuracy within a radius of 1,750 feet; and

(B) does not include—

(i) the content of communications; or

(ii) any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(23) PROCESS OR PROCESSING.—The term ''process'' or ''processing'' means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(24) PROCESSOR.—The term ''processor'' means a person that processes personal data on behalf of a controller.

(25) PROFILING.—The term ''profiling'' means any form of processing that is solely automated and performed on personal data to evaluate, analyze, or predict personal aspects of the economic situation, health, personal preference, interest, reliability, behavior, location, or movement of an identified or identifiable consumer.

(26) PSEUDONYMOUS DATA.—The term ''pseudonymous data'' means personal data that cannot be attributed to a specific individual without the use of additional information if the additional information is kept separately and is subject to appropriate administrative and technical measures to ensure that the personal data is not attributed to an identified or identifiable individual.

(27) PUBLICLY AVAILABLE INFORMATION.—The term ''publicly available information'' means information that is lawfully made available through Federal, State, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

(28) SALE OF PERSONAL DATA.—The term ''sale of personal data''—

(A) means the exchange of personal data for monetary consideration by the controller to another controller or to a governmental entity; and

(B) does not include—

(i) the disclosure of personal data to a processor that processes the personal data on behalf of the controller;

(ii) the disclosure of personal data to another controller for the purposes of providing a product or service requested by the consumer;

(iii) the disclosure or transfer of personal data to an affiliate of the controller;

(iv) the disclosure of information that the consumer intentionally made available to the public;

(v) the disclosure or transfer of personal data to another controller as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the new controller assumes control of any of the assets of the previous controller; or

(vi) the disclosure of personal data in the course of reporting, news-gathering, speaking, or other activities intended to inform the public on matters of public interest or public concern.

(29) SECRETARY.—The term ''Secretary'' means the Secretary of Commerce.

(30) SENSITIVE DATA.—The term ''sensitive data'' means a category of personal data that includes—

(A) personal data that discloses racial or ethnic origin, religious belief, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;

(B) genetic or biometric data that is processed for the purpose of uniquely identifying a specific individual;

(C) personal data collected from a child or teen; and

(D) precise geolocation data.

(31) STATE.—The term ''State'' means each State of the United States, the District of Columbia, each commonwealth, territory, or possession of the United States, and each federally recognized Indian Tribe.

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

(A) means to display an advertisement to a consumer in which the advertisement is selected based on personal data obtained from the activities of that consumer over time and across nonaffiliated websites or online applications to predict the preferences or interests of that consumer; and

(B) does not include—

(i) an advertisement based on activities within the website or online application of a controller;

(ii) an advertisement based on the context of a current search query, visit to a website, or online application of a consumer;

(iii) an advertisement directed to a consumer in response to the request for information or feedback by the consumer; or

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

(33) TEEN.—The term ''teen'' means an individual who is the age of 13 or over and under the age of 16.

(34) TRADE SECRET.—The term ''trade secret'' has the meaning given that term in section 1839 of title 18, United States Code.

(35) VERIFIABLE CONSENT.—The term ''verifiable consent'' means any reasonable effort (taking into consideration available technology) by a controller, including a request for authorization for future processing of personal data, to ensure that the parent of a teen—

(A) receives direct notice of the processing practices of the controller with respect to personal data; and

(B) before the personal data of the teen is collected, freely and unambiguously authorizes—

(i) the processing of the personal data; and

(ii) any subsequent use of the personal data.

SEC. 17. SEVERABILITY.

If any provision of this Act or the application of this Act to any person or circumstance is held invalid, the remaining provisions of this Act and the application of this Act to other persons or circumstances shall not be affected.

SEC. 18. EFFECTIVE DATES.

(a) IN GENERAL.—Except as provided in subsection (b), this Act shall take effect 2 years after the date of the enactment of this Act.

(b) EXCEPTIONS.—Notwithstanding subsection (a), sections 2, 4, and 5 shall take effect 1 year after the date of the enactment of this Act.