

.....
(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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Securing and Establishing Consumer Uniform Rights
6 and Enforcement over Data Act” or the “SECURE Data
7 Act”.

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

- Sec. 1. Short title.
- Sec. 2. Consumer privacy rights.
- Sec. 3. Controllers.
- Sec. 4. Data security.
- Sec. 5. Data brokers.
- Sec. 6. Processors.
- Sec. 7. Deidentified and pseudonymous data.
- Sec. 8. Codes of conduct.
- Sec. 9. Cross-border data flows.
- Sec. 10. Study on universal opt-out mechanisms.
- Sec. 11. Rules of construction.
- Sec. 12. Enforcement.
- Sec. 13. Applicability.
- Sec. 14. Relationship to Federal laws.
- Sec. 15. Relationship to State laws.
- Sec. 16. Definitions.
- Sec. 17. Severability.
- Sec. 18. Effective dates.

3 **SEC. 2. CONSUMER PRIVACY RIGHTS.**

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

6 (1) To confirm whether a controller is proc-
7 essing the personal data of the consumer and have
8 access to a copy of such data, unless the confirma-
9 tion and access would require the controller to reveal
10 a trade secret.

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

15 (3) To delete personal data provided by or ob-
16 tained about the consumer.

1 (4) If the data is available in a digital format
2 and to the extent technically feasible, to obtain a
3 copy of the personal data that the consumer pre-
4 viously provided to the controller in a portable and
5 readily usable format that allows the consumer to
6 transmit the data to another controller without hin-
7 drance.

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

10 (A) Targeted advertising.

11 (B) The sale of personal data.

12 (C) Reliance on profiling to make a deci-
13 sion that has a legal or similarly significant ef-
14 fect on the consumer.

15 (b) CONSENT REQUIRED FOR PROCESSING SEN-
16 SITIVE DATA.—

17 (1) IN GENERAL.—Except as provided in para-
18 graphs (2) and (3), a controller may not process the
19 sensitive data of a consumer without obtaining the
20 consent of the consumer before processing.

21 (2) APPLICABILITY TO A CHILD.—Notwith-
22 standing paragraph (1), a controller shall process
23 the sensitive data of a child in accordance with the
24 Children's Online Privacy Protection Act of 1998
25 (15 U.S.C. 6501 et seq).

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

5 (c) CONSUMER PRIVACY RIGHTS REQUESTS.—

6 (1) REQUEST FOR CONSUMER RIGHTS.—A con-
7 troller shall comply with any consumer privacy right
8 described in subsection (a) once a consumer submits
9 a request that specifies each consumer privacy right
10 the consumer requests to exercise and the controller
11 authenticates the consumer.

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

17 (d) CONTROLLER REQUIREMENTS.—

18 (1) DEADLINE FOR RESPONSE.—Except as pro-
19 vided in paragraph (2), without undue delay and not
20 later than 45 days after the date on which a con-
21 sumer submits a request under subsection (c), a con-
22 troller—

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

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

3 (i) the controller declines to take ac-
4 tion;

5 (ii) includes a justification for such
6 inaction; and

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

10 (2) EXTENSION OF RESPONSE PERIOD.—The
11 controller may extend the period described in para-
12 graph (1)(A) an additional 45 days when reasonably
13 necessary, taking into consideration the complexity
14 and number of requests submitted by the consumer,
15 if the controller informs the consumer of the exten-
16 sion during such period with the reason for such ex-
17 tension.

18 (3) FEES CHARGED.—

19 (A) FREE OF CHARGE.—For each con-
20 sumer privacy right described in subsection (a),
21 a consumer may submit to each controller 2 re-
22 quests under subsection (c) related to such con-
23 sumer privacy right in a year free of charge.

24 (B) REASONABLE FEE FOR ADMINISTRA-
25 TIVE COST.—If a consumer submits more than

1 2 such requests or submits a request that is
2 technically infeasible or manifestly unfounded,
3 the controller may—

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

10 (ii) decline to act on the request.

11 (C) CONTROLLER DOCUMENTATION RE-
12 QUIRED.—The controller shall demonstrate,
13 document, and provide to the Commission or a
14 State attorney general, upon request, any tech-
15 nically infeasible or manifestly unfounded na-
16 ture of any such request.

17 (4) AUTHENTICATION.—If a controller is un-
18 able to authenticate a consumer who submits a re-
19 quest under subsection (c), the controller is not re-
20 quired to comply with such request and may request
21 that the consumer provide additional information
22 reasonably necessary to authenticate the consumer
23 and the request.

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

1 about a consumer from a source other than the con-
2 sumer is considered to be in compliance with the re-
3 quest of a consumer under subsection (c) to delete
4 that personal data under subsection (a)(3) by—

5 (A) retaining a record of the deletion re-
6 quest and the minimum data necessary for the
7 purpose of ensuring the personal data of the
8 consumer remains deleted from the records of
9 the controller and not using the retained data
10 for any other purpose under this Act; or

11 (B) opting the consumer out of the proc-
12 essing of that personal data for any purpose
13 other than a purpose that is exempt under the
14 provisions of this Act.

15 (6) APPLICABILITY TO A CHILD.—With respect
16 to a request of a consumer under subsection (c) for
17 a child, a controller shall be deemed to be in compli-
18 ance with such subsection if the controller responds
19 to an equivalent consumer privacy right exercised by
20 a parent under the Children’s Online Privacy Pro-
21 tection Act of 1998 (15 U.S.C. 6501 et seq).

22 (e) APPEAL PROCESS.—

23 (1) ESTABLISHMENT OF PROCESS.—A con-
24 troller shall establish a process for a consumer to

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

3 (2) AVAILABILITY.—The appeal process estab-
4 lished pursuant to paragraph (1) shall be conspicu-
5 ously available and similar to the process for a re-
6 quest submitted under subsection (c).

7 (3) DEADLINE TO RESPOND.—Not later than
8 60 days after the date on which an appeal is re-
9 ceived by a controller, the controller—

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

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

19 (f) EXERCISING CONSUMER RIGHTS.—

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

1 (2) CONSIDERATIONS.—In establishing the
2 means pursuant to paragraph (1), a controller shall
3 take into account the ways in which a consumer nor-
4 mally interacts with the controller, the need for se-
5 cure and reliable communication of such requests,
6 and the ability of the controller to authenticate the
7 consumer making the request.

8 (3) NEW ACCOUNTS NOT REQUIRED.—A con-
9 troller may not require a consumer to create a new
10 account in order to exercise consumer privacy rights
11 described under subsection (a) but may require a
12 consumer to use an existing account.

13 **SEC. 3. CONTROLLERS.**

14 (a) DATA MINIMIZATION.—A controller shall limit
15 the collection of personal data to what is adequate, rel-
16 evant, and reasonably necessary in relation to each pur-
17 pose for which the data is processed as disclosed to the
18 consumer.

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

1 (c) CIVIL RIGHTS.—A controller may not process per-
2 sonal data in violation of a Federal law that prohibits un-
3 lawful discrimination against a consumer.

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

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

12 (1) to require a controller to provide a product
13 or service that requires the personal data of a con-
14 sumer that the controller does not collect or main-
15 tain; or

16 (2) to prohibit a controller from offering a dif-
17 ferent price, rate, level, quality, or selection of goods
18 or services to a consumer, including offering goods
19 or services for no fee, if the offer is related to the
20 voluntary participation of a consumer in a bona fide
21 loyalty, rewards, premium features, discounts, or
22 club card program.

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

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

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

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

10 (2) Each purpose for processing personal data.

11 (3) How a consumer may exercise a consumer
12 right described under section 2, including how a con-
13 sumer may appeal the decision of a controller under
14 section 2(d).

15 (4) Each category of personal data the con-
16 troller shares with any other controller or any gov-
17 ernmental entity.

18 (5) Each category of other controllers or any
19 governmental entity, if any, with whom the con-
20 troller shares personal data.

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

1 (h) DISCLOSURE OF SALE.—If a controller sells per-
2 sonal data of a consumer, the controller shall clearly and
3 conspicuously disclose—

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

6 (2) the manner in which a consumer may exer-
7 cise the right to opt out of the sale of such personal
8 data under section 2(a)(5).

9 (i) DISCLOSURE OF TARGETED ADVERTISING.—If a
10 controller processes personal data of a consumer for tar-
11 geted advertising, the controller shall clearly and conspicu-
12 ously disclose—

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

15 (2) the manner in which a consumer may exer-
16 cise the right to opt out of such processing under
17 section 2(a)(5).

18 (j) AUTOMATED DECISION MAKING.—

19 (1) PROFILING.—A controller that relies on
20 profiling to make a decision that has a legal or simi-
21 larly significant effect on a consumer shall clearly
22 and conspicuously disclose to such consumer before
23 any such decision is made that—

24 (A) the decision will be made using auto-
25 mated means; and

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

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

9 **SEC. 4. DATA SECURITY.**

10 (a) DATA SECURITY.—A controller shall establish,
11 implement, and maintain reasonable administrative, tech-
12 nical, and physical data security practices to protect the
13 confidentiality, integrity, and accessibility of personal data
14 and that are appropriate to the volume, sensitivity, and
15 nature of such personal data.

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

19 (1) the controller complies with a relevant code
20 of conduct approved under section 8(a)(3) (or a rel-
21 evant certification described in section 8(f)); or

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

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

1 and physical data security practices for the pro-
2 tection of the confidentiality, integrity, and ac-
3 cessibility of personal data, including such a
4 practice demonstrated by adherence to a widely-
5 accepted technical specification or through a
6 third-party attestation; and

7 (B) a comprehensive data security program
8 that reasonably conforms to a relevant Federal
9 or widely-accepted international risk manage-
10 ment framework for identifying and protecting
11 against data security risks, and for detecting,
12 responding to, and recovering from data secu-
13 rity events.

14 **SEC. 5. DATA BROKERS.**

15 (a) DISCLOSURE.—A data broker shall post on a pub-
16 licly available website or mobile application a conspicuous
17 notice that—

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

20 (2) is clear, not misleading, and readily acces-
21 sible by the public; and

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

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

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

5 (1) The legal name of the data broker.

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

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

11 (4) A statement of whether the data broker im-
12 plements a purchaser credentialing process.

13 (5) A description of any incident of unauthor-
14 ized access to personal data that the data broker has
15 reported to a Federal or State governmental entity
16 pursuant to an applicable law, rule, or regulation
17 during the year before the year in which the reg-
18 istration is filed, and if known, the total number of
19 consumers affected by each previously reported inci-
20 dent of such unauthorized access.

21 (6) A link to the privacy policy published in ac-
22 cordance with section 3(g).

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

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

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

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

11 (3) For each data broker, a link to a website
12 published by the data broker that informs a con-
13 sumer how to exercise any consumer right described
14 under section 2.

15 **SEC. 6. PROCESSORS.**

16 (a) ADHERENCE TO CONTROLLER INSTRUCTIONS.—
17 A processor shall adhere to the instructions of a controller
18 and shall assist the controller in meeting the requirements
19 of this Act, including by taking into account the nature
20 of processing and the information available to the proc-
21 essor—

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

1 assertion of any consumer right described under sec-
2 tion 2; and

3 (2) by assisting the controller in meeting the re-
4 quirements of the controller under section 4.

5 (b) CONTRACTUAL OBLIGATION.—A contract be-
6 tween a controller and a processor shall govern the data
7 processing procedures of the processor with respect to
8 processing performed on behalf of the controller. The con-
9 tract shall clearly set forth instructions for processing per-
10 sonal data, the nature and purpose of processing, the type
11 of personal data subject to processing, the duration of
12 processing, and the rights and obligations of both parties.

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

16 (1) Ensures that each person processing per-
17 sonal data is subject to a duty of confidentiality with
18 respect to the data.

19 (2) At the direction of the controller, deletes or
20 returns all personal data to the controller as re-
21 quested at the end of the provision of services, un-
22 less retention of the personal data is required by
23 law.

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

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

4 (4) Either—

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

8 (B) the processor—

9 (i) arranges for a qualified and inde-
10 pendent assessor to conduct an assessment
11 of the policies and administrative and tech-
12 nical measures of such processor that meet
13 the requirements of this Act using an ap-
14 propriate and accepted control standard or
15 framework and assessment procedure for
16 such assessment; and

17 (ii) provides a report of the assess-
18 ment to the controller upon request.

19 (5) If a processor engages a subcontractor, in-
20 clude in any subcontract a requirement that the sub-
21 contractor meet the obligations of the processor with
22 respect to the personal data.

23 (d) RULE OF CONSTRUCTION.—Nothing in this sec-
24 tion may be construed to relieve a controller or processor

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

3 (e) APPLICABILITY.—

4 (1) CONTROLLER OR PROCESSOR.—The deter-
5 mination about whether a person is acting as a con-
6 troller or processor with respect to a specific proc-
7 essing of personal data is a fact-based determination
8 that depends upon the context in which personal
9 data is to be processed.

10 (2) CONTROLLER.—If a processor, alone or
11 jointly with others, begins determining the purpose
12 and means of processing personal data, such proc-
13 essor is a controller with respect to a specific proc-
14 essing of such personal data.

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

18 **SEC. 7. DEIDENTIFIED AND PSEUDONYMOUS DATA.**

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

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

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

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

4 (b) ONGOING COMPLIANCE.—A controller that dis-
5 closes deidentified or pseudonymous data shall exercise
6 reasonable oversight to monitor compliance with any con-
7 tractual commitment to which the deidentified or pseudon-
8 ymous data is subject and shall take appropriate steps to
9 address any breach of such contractual commitment.

10 (c) PSEUDONYMOUS DATA.—An assertion of any con-
11 sumer right described under section 2 does not apply to
12 pseudonymous data for a case in which the controller is
13 able to demonstrate any information necessary to identify
14 the consumer is kept separately and is subject to appro-
15 priate administrative and technical measures to ensure
16 that the personal data is not attributed to an identified
17 or identifiable natural person.

18 (d) RULE OF CONSTRUCTION RELATING TO
19 DEIDENTIFIED OR PSEUDONYMOUS DATA.—Nothing in
20 this Act may be construed to require a controller or proc-
21 essor to—

22 (1) re-identify deidentified data or pseudony-
23 mous data; or

24 (2) maintain data in identifiable form, or col-
25 lect, obtain, retain, or access any data or technology,

1 in order to be capable of associating a consumer re-
2 quest with personal data.

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

8 (1) the controller is not reasonably capable of
9 associating the request with the personal data or it
10 would be unduly burdensome for the controller to as-
11 sociate the request with the personal data;

12 (2) the controller does not use the personal
13 data to recognize or respond to the specific con-
14 sumer who is the subject of the personal data, or as-
15 sociate the personal data with other personal data
16 about the same specific consumer; and

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

22 **SEC. 8. CODES OF CONDUCT.**

23 (a) APPLICATION FOR APPROVAL OF CODE OF CON-
24 DUCT.—

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

7 (2) APPLICATION REQUIREMENTS.—An applica-
8 tion submitted under paragraph (1) shall include the
9 following:

10 (A) A description of the specific require-
11 ments of this Act to which the code of conduct
12 proposed in the application will apply.

13 (B) A description of how the code of con-
14 duct will meet or exceed such requirements.

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

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

20 (E) A description of the independent orga-
21 nization that will administer the code of con-
22 duct with respect to controllers or processors,
23 including an explanation of how the inde-
24 pendent organization is governed.

1 (F) A description of how the entities de-
2 scribed in subparagraph (C) will be assessed for
3 compliance with the code of conduct by the
4 independent organization described in subpara-
5 graph (E).

6 (G) A description of how the independent
7 organization will refer to the Commission or to
8 a State attorney general any controller or proc-
9 essor that does not—

10 (i) meet the requirements of this Act;

11 or

12 (ii) meet or exceed the requirements
13 of the Act in accordance with the certifi-
14 cation publicly disclosed by the controller
15 or processor under subsection (c).

16 (3) REVIEW BY SECRETARY.—

17 (A) INITIAL APPROVAL.—

18 (i) PUBLIC COMMENT PERIOD.—Not
19 later than 90 days after the date on which
20 the Secretary receives an application sub-
21 mitted under paragraph (1), the Secretary
22 shall publish the application and provide
23 an opportunity for public comment on the
24 code of conduct proposed in the applica-
25 tion.

1 (ii) APPROVAL CRITERIA.—The Sec-
2 retary, in consultation with the Commis-
3 sion, shall approve an application sub-
4 mitted under paragraph (1), including the
5 independent organization that will admin-
6 ister the code of conduct, if the controller
7 or processor (or the group of controllers or
8 processors) that submits the application
9 demonstrates that the code of conduct pro-
10 posed in the application meets the fol-
11 lowing criteria:

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

14 (II) Provides for regular review
15 and validation by the independent or-
16 ganization to ensure that the con-
17 troller or processor (or the group of
18 controllers or processors) that com-
19 plies with the code of conduct con-
20 tinues to meet or exceed the relevant
21 requirements of this Act.

22 (III) Includes referral to the
23 Commission for enforcement or refer-
24 ral to the appropriate State attorney
25 general for enforcement.

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

8 (B) APPROVAL OF MODIFICATIONS.—

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

14 (I) the independent organization
15 shall submit to the Secretary an appli-
16 cation for approval of the significant
17 updates made to the code of conduct;
18 and

19 (II) not later than 90 days after
20 the date on which the Secretary re-
21 ceives an application for an updated
22 code of conduct submitted under sub-
23 clause (I), the Secretary shall publish
24 the proposed updated code of conduct

1 and provide an opportunity for public
2 comment.

3 (ii) **TIMELINE.**—Not later than 180
4 days after the date on which the Secretary
5 receives an application for an updated code
6 of conduct submitted under clause (i)(I),
7 the Secretary, considering the approval cri-
8 teria described in subparagraph (A)(ii),
9 shall issue a public determination approv-
10 ing or denying the application and pro-
11 viding the reasons for such approval or de-
12 nial.

13 (b) **WITHDRAWAL OF APPROVAL.**—

14 (1) **IN GENERAL.**—If the Secretary has clear
15 and convincing evidence that a code of conduct ap-
16 proved under subsection (a)(3) no longer meets the
17 relevant requirements of this Act or that compliance
18 with the code of conduct is insufficiently assessed by
19 the independent organization that administers the
20 code of conduct, the Secretary shall notify the rel-
21 evant controller or processor (or the relevant group
22 of controllers or processors) and the independent or-
23 ganization of a potential withdrawal of approval by
24 the Secretary and of the opportunity to cure any al-
25 leged deficiency under paragraph (2).

1 (2) OPPORTUNITY TO CURE.—

2 (A) IN GENERAL.—Not later than 180
3 days after the date on which a controller or
4 processor (or a group of controllers or proc-
5 essors) receives the notice described in para-
6 graph (1), the controller or processor (or the
7 group of controllers or processors) and the rel-
8 evant independent organization may—

9 (i) create a proposed cure to any al-
10 leged deficiency of the code of conduct or
11 the enforcement of the code of conduct;
12 and

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

15 (B) REVIEW OF PROPOSED CURE.—If the
16 Secretary determines within 60 days that a pro-
17 posed cure submitted under subparagraph
18 (A)(ii) eliminates an alleged deficiency of the
19 code of conduct or the assessment of compli-
20 ance with the code of conduct, the Secretary
21 may not withdraw the approval of such code of
22 conduct on the basis of such deficiency.

23 (3) WITHDRAWAL OF APPROVAL.—

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

1 under subparagraph (A)(ii) does not eliminate
2 an alleged deficiency of the code of conduct or
3 the assessment of compliance with the code of
4 the conduct, the Secretary may withdraw ap-
5 proval of such code of conduct on the basis of
6 such deficiency.

7 (B) NOTIFICATION.—Not later than 10
8 days after the date on which the Secretary
9 makes a determination under subparagraph
10 (A), the Secretary shall notify the relevant con-
11 troller or processor (or the relevant group of
12 controllers or processors) and the independent
13 organization of the relevant withdrawal of ap-
14 proval described in subparagraph (A).

15 (C) EFFECT.—A withdrawal of approval
16 described in subparagraph (A) shall take effect
17 on the date that is 30 days after the date on
18 which the Secretary provides the notification re-
19 quired by subparagraph (B).

20 (D) PUBLICATION.—Not later than 30
21 days after the date on which the Secretary pro-
22 vides notification required by subparagraph (B,
23 the Secretary shall publish on a publicly avail-
24 able website a notice about the relevant with-

1 drawal of approval described in subparagraph
2 (A).

3 (c) PUBLIC DISCLOSURE.—A controller or processor
4 that participates in a code of conduct approved under sub-
5 section (a)(3) shall certify on a publicly available website
6 that the controller or processor is in compliance with the
7 code of conduct, including by listing the independent orga-
8 nization that administers the code of conduct.

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

16 (e) CODES OF CONDUCT FOR SMALL BUSINESSES.—

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

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

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

3 (B) solicit independent organizations to ad-
4 minister the codes of conduct.

5 (3) REQUIREMENTS FOR CODE OF CONDUCT.—

6 A code of conduct published under paragraph (1)
7 shall meet the following requirements:

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

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

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

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

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

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

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

6 **SEC. 9. CROSS-BORDER DATA FLOWS.**

7 (a) **PRINCIPAL ADVISOR.**—The Secretary shall serve
8 as the principal advisor to the President on policy relating
9 to the international flow of personal data and the protec-
10 tion of personal data in international commerce.

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

15 (1) Assessing the laws, regulations, require-
16 ments, frameworks, and practices (and the imple-
17 mentation thereof) of foreign governments for—

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

21 (B) any impact on consumers and busi-
22 nesses in the United States, including with re-
23 spect to economic competitiveness, innovation,
24 and data security; and

1 (C) any impact on the economic and secu-
2 rity interests of the United States.

3 (2) Developing policy and recommendations re-
4 lating to—

5 (A) identifying the benefits of the inter-
6 national flow of personal data to consumers and
7 businesses, including economic competitiveness,
8 innovation, and data security;

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

15 (C) promoting the protection of personal
16 data in a manner that maintains the inter-
17 national flow of personal data in international
18 commerce; and

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

23 (3) Establishing, maintaining, and promoting
24 frameworks, certifications, principles, and partner-
25 ships to facilitate the international flow of personal

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

3 (4) Coordinating with any relevant agency as
4 needed.

5 (c) INTERNATIONAL COOPERATION.—

6 (1) AUTHORITY TO ENTER AGREEMENT.—The
7 Secretary, as the Secretary determines appropriate,
8 may enter into an agreement with a foreign govern-
9 ment, international forum, or foreign political or
10 economic union to promote the international flow of
11 personal data and the protection of personal data in
12 international commerce.

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

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

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

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

1 (d) RULE OF CONSTRUCTION.—Nothing in this sec-
2 tion may be construed to alter the authority of any agency
3 with rulemaking and enforcement authority under subtitle
4 A of title V of the Gramm-Leach-Bliley Act (15 U.S.C.
5 6801 et seq.).

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

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

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

12 (2) reviews commercially available technologies,
13 including a web browser setting or extension or a
14 global setting on an electronic device, that allow a
15 consumer to opt out of the processing of the per-
16 sonal data of the consumer by a controller;

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

21 (4) limits such review and consideration in ac-
22 cordance with the scope of this Act.

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

1 to the study required by subsection (a) shall meet the fol-
2 lowing requirements:

3 (1) Shall require a consumer to make an af-
4 firmative, freely given, and unambiguous choice to
5 indicate the intent of the consumer to opt out of any
6 processing of the personal data of the consumer by
7 a controller.

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

10 (3) May not unduly burden lawful data proc-
11 essing by a controller or processor, including with
12 respect to beneficial uses of personal data.

13 **SEC. 11. RULES OF CONSTRUCTION.**

14 (a) IN GENERAL.—Nothing in this Act may be con-
15 strued to restrict the ability of a controller or processor
16 to do any of the following:

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

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

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

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

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

11 (6) Prevent, detect, protect against, or respond
12 to a security incident, including a data security inci-
13 dent, identity theft, fraud, harassment, malicious or
14 deceptive activity, or any other similar illegal activ-
15 ity.

16 (7) Preserve the integrity or security of sys-
17 tems.

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

20 (9) Engage in public or peer-reviewed scientific
21 or statistical research in the public interest that ad-
22 heres to any applicable Federal or State ethics or
23 privacy law and is approved, monitored, and gov-
24 erned by an institutional review board (or similar

1 independent oversight entity) that considers the fol-
2 lowing:

3 (A) If the deletion of the personal data of
4 a consumer is likely to provide substantial bene-
5 fits that do not exclusively accrue to the con-
6 troller.

7 (B) If the controller has implemented rea-
8 sonable safeguards to mitigate privacy and data
9 security risks to a consumer associated with re-
10 search, including any risks associated with re-
11 identification of the personal data of the con-
12 sumer.

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

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

19 (1) Conduct internal research to develop, im-
20 prove, or repair a product, service, or technology.

21 (2) Effectuate a product recall.

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

25 (4) Perform an internal operation that—

1 (A) is reasonably aligned with the expecta-
2 tions of a consumer;

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

6 (C) is otherwise compatible with processing
7 data to—

8 (i) provide a product or service spe-
9 cifically requested by a consumer or a par-
10 ent of a consumer (if the consumer is a
11 child or teen); or

12 (ii) perform a contract to which a con-
13 sumer or a parent of a consumer (if the
14 consumer is a child or teen) is a party.

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

20 (d) PROTECTED DISCLOSURE.—A controller or proc-
21 essor that discloses the personal data of a consumer to
22 another controller or processor in compliance with the re-
23 quirements of this Act does not violate this Act if the con-
24 troller or processor that receives and processes such per-
25 sonal data violates this Act if, at the time of disclosing

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

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

12 **SEC. 12. ENFORCEMENT.**

13 (a) ENFORCEMENT BY COMMISSION.—

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

20 (2) POWERS OF COMMISSION.—Except as pro-
21 vided in paragraphs (3) and (4), the Commission
22 shall enforce this Act in the same manner, by the
23 same means, and with the same jurisdiction, powers,
24 and duties as though all applicable terms and provi-
25 sions of the Federal Trade Commission Act (15

1 U.S.C. 41 et seq.) were incorporated into and made
2 a part of this Act, and any person who violates this
3 Act shall be subject to the penalties and entitled to
4 the privileges and immunities provided in the Fed-
5 eral Trade Commission Act.

6 (3) COMMON CARRIERS.—Notwithstanding sec-
7 tion 4, 5(a)(2), or 6 of the Federal Trade Commis-
8 sion Act (15 U.S.C. 44; 45(a)(2); 46) or any juris-
9 dictional limitation of the Federal Trade Commis-
10 sion, the Federal Trade Commission shall also en-
11 force this Act, in the same manner provided in para-
12 graphs (1) and (2), with respect to common carriers
13 subject to the Communications Act of 1934 (47
14 U.S.C. 151 et seq.).

15 (4) CIVIL RIGHTS VIOLATIONS.—

16 (A) EXCEPTION.—Notwithstanding para-
17 graphs (1), (2), and (3), the Commission may
18 not enforce any violation of section 3(c) of this
19 Act.

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

1 ment action or proceeding relating to the al-
2 leged violation described in the information.

3 (b) ACTIONS BY STATES.—

4 (1) IN GENERAL.—In any case in which the at-
5 torney general of a State has reason to believe that
6 an interest of the residents of such State has been
7 or is threatened or adversely affected by an act or
8 practice in violation of this Act, the attorney gen-
9 eral, as *parens patriae*, may bring a civil action on
10 behalf of the residents of the State in an appropriate
11 district court of the United States to—

12 (A) enjoin such act or practice;

13 (B) enforce compliance with this Act;

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

17 (D) obtain such other legal and equitable
18 relief as the court may consider to be appro-
19 priate.

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

1 graph before the filing of the action, the attorney
2 general shall provide written notice of the action and
3 a copy of the complaint to the Commission imme-
4 diately upon the filing of the action.

5 (3) AUTHORITY OF COMMISSION.—

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

10 (i) to intervene in the action;

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

13 (iii) to file petitions for appeal.

14 (B) LIMITATION ON STATE ACTION WHILE
15 FEDERAL ACTION IS PENDING.—If the Commis-
16 sion or the Attorney General of the United
17 States has instituted a civil action for violation
18 of this Act (referred to in this subparagraph as
19 the “Federal action”), no State attorney gen-
20 eral may bring an action under this subsection
21 during the pendency of the Federal action
22 against any defendant named in the complaint
23 in the Federal action for any violation of this
24 Act alleged in such complaint.

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

9 (c) RIGHT TO CURE.—

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

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

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

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

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

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

13 (A) fails to cure the alleged violation pur-
14 suant to paragraph (2); or

15 (B) after curing the alleged violation pur-
16 suant to paragraph (2), continues to violate this
17 Act.

18 **SEC. 13. APPLICABILITY.**

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

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

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

4 (B) processes or engages in the sale of per-
5 sonal data of a resident of the United States;
6 and

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

9 (A) collects and processes personal data of
10 more than 200,000 consumers annually (exclud-
11 ing personal data controlled or processed solely
12 for the purpose of completing a payment trans-
13 action) and has an annual gross revenue of
14 \$25,000,000 or more (as adjusted on January
15 1 each year by the percentage increase (if any),
16 during the preceding 12-month period, in the
17 Consumer Price Index for All Urban Con-
18 sumers published by the Bureau of Labor Sta-
19 tistics); or

20 (B) collects and processes personal data of
21 100,000 or more consumers annually (excluding
22 personal data controlled or processed solely for
23 the purpose of completing a payment trans-
24 action) and derives 25 percent or more of the

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

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

5 (1) A Federal, State, or local governmental en-
6 tity.

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

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

15 (4) A covered entity or business associate sub-
16 ject to parts 160 and 164 of title 45, Code of Fed-
17 eral Regulations.

18 (5) A nonprofit organization.

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

24 (7) An institution of higher education.

1 (8) The National Center for Missing and Ex-
2 ploited Children.

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

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

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

12 (12) Data processed or maintained—

13 (A) by an individual applying to, employed
14 by, or acting as an agent or independent con-
15 tractor of a controller or processor for such ap-
16 plication, employment, or action;

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

19 (C) that is necessary for the administra-
20 tion of benefits for an individual.

21 (13) The following information:

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

25 (B) Health records.

1 (C) Records relating to the identity, diag-
2 nosis, prognosis, or treatment of a patient
3 under section 543 of the Public Health Service
4 Act (42 U.S.C. 290dd-2).

5 (D) Data, information, or identifiable pri-
6 vate information (as such term is defined in
7 section 46.102 of title 45, Code of Federal Reg-
8 ulations) obtained pursuant to any of the fol-
9 lowing:

10 (i) Part 46 of title 45, Code of Fed-
11 eral Regulations.

12 (ii) The Guideline for Good Clinical
13 Practice E6(R3) issued by The Inter-
14 national Council for Harmonisation of
15 Technical Requirements for Pharma-
16 ceuticals for Human Use.

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

19 (E) Information reported pursuant to the
20 Health Care Quality Improvement Act of 1986
21 (42 U.S.C. 11101 et seq.).

22 (F) Identifiable patient safety work prod-
23 uct and nonidentifiable patient safety work
24 product (as such terms are defined in section
25 921 of the Public Health Service Act (42

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

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

9 (H) Information that is included in a lim-
10 ited data set in accordance with the standards
11 and specifications under section 164.514(e) of
12 title 45, Code of Federal Regulations.

13 (I) Personal data that—

14 (i) may impact the creditworthiness,
15 credit standing, credit capacity, character,
16 general reputation, personal characteris-
17 ties, or mode of living of a consumer; and

18 (ii) is collected or disclosed by a con-
19 sumer reporting agency (as such term is
20 defined in section 603(f) of the Fair Credit
21 Reporting Act (15 U.S.C. 1681a(f))) or a
22 furnisher, to the extent that the consumer
23 reporting agency or furnisher is engaged in
24 activities subject to the Fair Credit Re-
25 porting Act.

1 (J) Personal information (as such term is
2 defined in section 2725 of title 18, United
3 States Code) collected, processed, sold, or dis-
4 closed under section 2721 of title 18, United
5 States Code.

6 (K) Personally identifiable information and
7 personally identifiable data regulated in accord-
8 ance with section 444 of the General Education
9 Provisions Act (commonly known as the “Fam-
10 ily Educational Rights and Privacy Act of
11 1974”) (20 U.S.C. 1232g).

12 (L) Personal data collected, processed,
13 sold, or disclosed as a result of an activity au-
14 thorized under the Farm Credit Act of 1971
15 (12 U.S.C. 2001 et seq.).

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

19 (N) Any information that originates from,
20 is intermingled with, or is treated in the same
21 manner as information described in subpara-
22 graphs (A) through (M) that is maintained by
23 the following:

24 (i) A covered entity or business asso-
25 ciate.

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

5 **SEC. 14. RELATIONSHIP TO FEDERAL LAWS.**

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

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

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

13 (3) Part C of title XI of the Social Security Act
14 (42 U.S.C. 1320d et seq.).

15 (4) Subtitle D of the HITECH Act (42 U.S.C.
16 17921 et seq.).

17 (5) Any regulations promulgated under section
18 264(c) of HIPAA (42 U.S.C. 1320d–2 note).

19 (6) The requirements regarding the confiden-
20 tiality of substance use disorder information under
21 section 543 of the Public Health Service Act (42
22 U.S.C. 290dd–2) or any regulation promulgated
23 under such section.

24 (7) The Fair Credit Reporting Act (15 U.S.C.
25 1681 et seq.).

1 (8) Section 444 of the General Education Pro-
2 visions Act (commonly known as the “Family Edu-
3 cational Rights and Privacy Act of 1974”) (20
4 U.S.C. 1232g) and part 99 of title 34, Code of Fed-
5 eral Regulations (or any successor regulation), to
6 the extent a controller or processor is an educational
7 agency or institution (as such term is defined in
8 99.3 of such title (or any successor regulation)).

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

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

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

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

18 (b) RELATIONSHIP TO COMMUNICATIONS ACT OF
19 1934.—

20 (1) IN GENERAL.—Except as provided in para-
21 graph (2), the Communications Act of 1934 (47
22 U.S.C. 151 et seq.), and any regulation promulgated
23 by the Federal Communications Commission pursu-
24 ant to such Act, shall not apply to a controller or

1 processor with respect to the collection, use, proc-
2 essing, transferring, or security of personal data.

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

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

8 **SEC. 15. RELATIONSHIP TO STATE LAWS.**

9 No State or political subdivision of a State may pre-
10 scribe, maintain, or enforce any law, rule, regulation, re-
11 quirement, standard, or other provision having the force
12 and effect of law, if such law, rule, regulation, require-
13 ment, standard, or other provision relates to the provisions
14 of this Act.

15 **SEC. 16. DEFINITIONS.**

16 In this Act:

17 (1) AFFILIATE.—

18 (A) IN GENERAL.—The term “affiliate”
19 means a legal entity that controls, is controlled
20 by, or is under common control with another
21 legal entity or shares common branding with
22 another legal entity.

23 (B) CONTROL; CONTROLLED.—In subpara-
24 graph (A), the terms “control” and “con-
25 trolled” mean—

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

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

8 (iii) the power to exercise controlling
9 influence over the management of a com-
10 pany.

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

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

20 (4) BIOMETRIC DATA.—The term “biometric
21 data”—

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

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

3 (B) does not include a physical or digital
4 photograph, a video or audio recording (or data
5 generated therefrom), or information collected,
6 used, or stored for health care treatment, pay-
7 ment, or operations pursuant to HIPAA.

8 (5) BUSINESS ASSOCIATE; COVERED ENTITY;
9 HEALTHCARE PROVIDER; PROTECTED HEALTH IN-
10 FORMATION.—The terms “business associate”, “cov-
11 ered entity”, “healthcare provider”, and “protected
12 health information” have the meanings given those
13 terms in for purposes of regulations promulgated
14 pursuant to section 264(c) of the Health Insurance
15 Portability and Accountability Act (42 U.S.C.
16 1320d–2 note).

17 (6) CHILD.—The term “child” means an indi-
18 vidual who is under the age of 13.

19 (7) COMMISSION.—The term “Commission”
20 means the Federal Trade Commission.

21 (8) CONSENT.—The term “consent”—

22 (A) means a clear affirmative act that sig-
23 nifies the freely given, specific, informed, and
24 unambiguous agreement by a consumer to proc-
25 ess personal data relating to the consumer; and

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

4 (9) CONSUMER.—The term “consumer”
5 means—

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

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

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

14 (11) COVERED NATION.—The term “covered
15 nation” has the meaning given that term in section
16 4872(f) of title 10, United States Code.

17 (12) DATA BROKER.—

18 (A) IN GENERAL.—The term “data
19 broker” means a controller that meets the fol-
20 lowing—

21 (i) The controller collects and proc-
22 esses personal data concerning a consumer
23 who is not:

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

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

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

7 (B) LIMITATION.—The term “data
8 broker” does not include a person acting as a
9 processor.

10 (13) DECISION THAT HAS A LEGAL OR SIMI-
11 LARLY SIGNIFICANT EFFECT.—The term “decision
12 that has a legal or similarly significant effect”
13 means a decision made by a controller about a con-
14 sumer to deny one of the following to the consumer:

15 (A) A healthcare service (as defined in
16 part 318.2 of title 16, Code of Federal Regula-
17 tions).

18 (B) A rental or lease of housing.

19 (C) An employment opportunity.

20 (14) DEIDENTIFIED DATA.—The term
21 “deidentified data” means data that cannot reason-
22 ably be linked to an identified or identifiable indi-
23 vidual or a device linked to an individual.

24 (15) HEALTH RECORD.—The term “health
25 record” means a record, other than for financial or

1 billing purposes, relating to an individual, kept by a
2 health care provider as a result of the professional
3 relationship established between the health care pro-
4 vider and the individual.

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

8 (17) IDENTIFIED OR IDENTIFIABLE NATURAL
9 PERSON.—The term “identified or identifiable nat-
10 ural person” means a person who can be readily
11 identified, directly or indirectly.

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

16 (19) NONPROFIT ORGANIZATION.—The term
17 “nonprofit organization” means an organization that
18 is described in section 501(c)(3) of the Internal Rev-
19 enue Code of 1986 and exempt from taxation under
20 section 501(a) of such Code.

21 (20) PARENT.—The term “parent”, with re-
22 spect to a child or teen, means an adult with the
23 legal right to make decisions on behalf of the child
24 or teen, including—

25 (A) a natural parent;

1 (B) an adoptive parent;

2 (C) a legal guardian; and

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

5 (21) PERSONAL DATA.—The term “personal
6 data”—

7 (A) means any information that is linked
8 or reasonably linkable to an identified or identi-
9 fiable natural person; and

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

12 (22) PRECISE GEOLOCATION DATA.—The term
13 “precise geolocation data”—

14 (A) means information derived from tech-
15 nology, including global positioning system level
16 latitude and longitude coordinates or other
17 mechanisms, that directly identifies the specific
18 location of a natural person with precision and
19 accuracy within a radius of 1,750 feet; and

20 (B) does not include—

21 (i) the content of communications; or

22 (ii) any data generated by or con-
23 nected to advanced utility metering infra-
24 structure systems or equipment for use by
25 a utility.

1 (23) PROCESS OR PROCESSING.—The term
2 “process” or “processing” means any operation or
3 set of operations performed, whether by manual or
4 automated means, on personal data or on sets of
5 personal data, such as the collection, use, storage,
6 disclosure, analysis, deletion, or modification of per-
7 sonal data.

8 (24) PROCESSOR.—The term “processor”
9 means a person that processes personal data on be-
10 half of a controller.

11 (25) PROFILING.—The term “profiling” means
12 any form of processing that is solely automated and
13 performed on personal data to evaluate, analyze, or
14 predict personal aspects of the economic situation,
15 health, personal preference, interest, reliability, be-
16 havior, location, or movement of an identified or
17 identifiable consumer.

18 (26) PSEUDONYMOUS DATA.—The term “pseu-
19 donymous data” means personal data that cannot be
20 attributed to a specific individual without the use of
21 additional information if the additional information
22 is kept separately and is subject to appropriate ad-
23 ministrative and technical measures to ensure that
24 the personal data is not attributed to an identified
25 or identifiable individual.

1 (27) PUBLICLY AVAILABLE INFORMATION.—

2 The term “publicly available information” means in-
3 formation that is lawfully made available through
4 Federal, State, or local government records, or infor-
5 mation that a business has a reasonable basis to be-
6 lieve is lawfully made available to the public through
7 widely distributed media, by the consumer, or by a
8 person to whom the consumer has disclosed the in-
9 formation, unless the consumer has restricted the in-
10 formation to a specific audience.

11 (28) SALE OF PERSONAL DATA.—The term
12 “sale of personal data”—

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

17 (B) does not include—

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

21 (ii) the disclosure of personal data to
22 another controller for the purposes of pro-
23 viding a product or service requested by
24 the consumer;

1 (iii) the disclosure or transfer of per-
2 sonal data to an affiliate of the controller;

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

6 (v) the disclosure or transfer of per-
7 sonal data to another controller as an asset
8 that is part of a merger, acquisition, bank-
9 ruptcy, or other transaction in which the
10 new controller assumes control of any of
11 the assets of the previous controller; or

12 (vi) the disclosure of personal data in
13 the course of reporting, news-gathering,
14 speaking, or other activities intended to in-
15 form the public on matters of public inter-
16 est or public concern.

17 (29) SECRETARY.—The term “Secretary”
18 means the Secretary of Commerce.

19 (30) SENSITIVE DATA.—The term “sensitive
20 data” means a category of personal data that in-
21 cludes—

22 (A) personal data that discloses racial or
23 ethnic origin, religious belief, mental or physical
24 health diagnosis, sexual orientation, or citizen-
25 ship or immigration status;

1 (B) genetic or biometric data that is proc-
2 essed for the purpose of uniquely identifying a
3 specific individual;

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

6 (D) precise geolocation data.

7 (31) STATE.—The term “State” means each
8 State of the United States, the District of Columbia,
9 each commonwealth, territory, or possession of the
10 United States, and each federally recognized Indian
11 Tribe.

12 (32) TARGETED ADVERTISING.—The term “tar-
13 geted advertising”—

14 (A) means to display an advertisement to
15 a consumer in which the advertisement is se-
16 lected based on personal data obtained from the
17 activities of that consumer over time and across
18 nonaffiliated websites or online applications to
19 predict the preferences or interests of that con-
20 sumer; and

21 (B) does not include—

22 (i) an advertisement based on activi-
23 ties within the website or online application
24 of a controller;

1 (ii) an advertisement based on the
2 context of a current search query, visit to
3 a website, or online application of a con-
4 sumer;

5 (iii) an advertisement directed to a
6 consumer in response to the request for in-
7 formation or feedback by the consumer; or

8 (iv) processing personal data proc-
9 essed solely for measuring or reporting ad-
10 vertising or content performance, reach, or
11 frequency, including independent measure-
12 ment.

13 (33) TEEN.—The term “teen” means an indi-
14 vidual who is the age of 13 or over and under the
15 age of 16.

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

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

1 (A) receives direct notice of the processing
2 practices of the controller with respect to per-
3 sonal data; and

4 (B) before the personal data of the teen is
5 collected, freely and unambiguously author-
6 izes—

7 (i) the processing of the personal
8 data; and

9 (ii) any subsequent use of the per-
10 sonal data.

11 **SEC. 17. SEVERABILITY.**

12 If any provision of this Act or the application of this
13 Act to any person or circumstance is held invalid, the re-
14 maining provisions of this Act and the application of this
15 Act to other persons or circumstances shall not be af-
16 fected.

17 **SEC. 18. EFFECTIVE DATES.**

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

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