

116TH CONGRESS
1ST SESSION

S. 1214

To establish and protect individual and collective privacy rights, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 11, 2019

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

A BILL

To establish and protect individual and collective privacy rights, 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; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Privacy Bill of Rights Act”.

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

- Sec. 1. Short title; table of contents.
- Sec. 2. Definitions.
- Sec. 3. Act prohibited.
- Sec. 4. Right to notice.
- Sec. 5. Right to control.
- Sec. 6. Right to access, correction, deletion, and data portability.
- Sec. 7. Prohibition on re-identifying personal information.

- Sec. 8. Prohibition on take-it-or-leave-it.
- Sec. 9. Prohibition on financial incentives.
- Sec. 10. Prohibition on disclosing information to third parties without proper assurances.
- Sec. 11. Use limitations.
- Sec. 12. Data minimization.
- Sec. 13. Right to data security.
- Sec. 14. Privacy and security officer.
- Sec. 15. Federal enforcement.
- Sec. 16. State enforcement.
- Sec. 17. Private right of action.
- Sec. 18. Relation to other laws.
- Sec. 19. Effective date.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) **BREACH OF SECURITY.**—The term “breach
4 of security” means any instance in which a person,
5 without authorization or in violation of any author-
6 ization provided to the person, gains access to, uses,
7 or discloses personal information.

8 (2) **COMMISSION.**—The term “Commission”
9 means the Federal Trade Commission.

10 (3) **COVERED ENTITY.**—The term “covered en-
11 tity” means any person that collects or otherwise ob-
12 tains personal information.

13 (4) **DATA BROKER.**—The term “data broker”
14 means a commercial entity that collects, assembles,
15 or maintains personal information concerning an in-
16 dividual who is not a customer or employee of the
17 entity, and who has not established a subscription or
18 account with the entity, in order to sell the informa-
19 tion or provide third-party access to the information.

1 (5) DE-IDENTIFIED.—The term “de-identified”,
 2 with respect to information, means information that
 3 cannot reasonably identify, relate to, describe, or be
 4 capable of being associated with or linked to, directly
 5 or indirectly, a particular individual.

6 (6) DISCLOSE.—The term “disclose” means to
 7 disclose, release, transfer, share, disseminate, make
 8 available, or otherwise communicate orally, in writ-
 9 ing, electronically, or by any other means to any
 10 third party.

11 (7) MINOR.—The term “minor” means any in-
 12 dividual who is under 16 years of age.

13 (8) MOBILE APPLICATION.—The term “mobile
 14 application” means a software program that runs on
 15 the operating system of a mobile device.

16 (9) OPT-IN APPROVAL.—The term “opt-in ap-
 17 proval” means affirmative, express consent of an in-
 18 dividual for a covered entity to use, disclose, or per-
 19 mit access to the individual’s personal information
 20 after the individual has received explicit notification
 21 of the request of the covered entity with respect to
 22 that information.

23 (10) PERSONAL INFORMATION.—

24 (A) IN GENERAL.—The term “personal in-
 25 formation” means information that directly or

1 indirectly identifies, relates to, describes, is ca-
2 pable of being associated with, or could reason-
3 ably be linked to, a particular individual.

4 (B) EXAMPLES.—The term “personal in-
5 formation” includes—

6 (i) an identifier such as a real name,
7 alias, signature, date of birth, gender iden-
8 tity, sexual orientation, marital status,
9 physical characteristic or description, post-
10 al address, telephone number, unique per-
11 sonal identifier, military identification
12 number, online identifier, Internet Protocol
13 address, email address, account name,
14 mother’s maiden name, social security
15 number, driver’s license number, passport
16 number, or other similar identifier;

17 (ii) information such as employment,
18 employment history, bank account number,
19 credit card number, debit card number, in-
20 surance policy number, or any other finan-
21 cial information, medical information, men-
22 tal health information, or health insurance
23 information;

24 (iii) commercial information, including
25 a record of personal property, income, as-

1 sets, leases, rentals, products or services
2 purchased, obtained, or considered, or
3 other purchasing or consuming history;

4 (iv) biometric information, including a
5 retina or iris scan, fingerprint, voiceprint,
6 or scan of hand or face geometry;

7 (v) internet or other electronic net-
8 work activity information, including brows-
9 ing history, search history, content, includ-
10 ing text, photographs, audio or video re-
11 cordings, or other user generated-content,
12 non-public communications, and informa-
13 tion regarding an individual's interaction
14 with an internet website, mobile applica-
15 tion, or advertisement;

16 (vi) historical or real-time geolocation
17 data;

18 (vii) audio, electronic, visual, thermal,
19 olfactory, or similar information;

20 (viii) education records, as defined in
21 section 99.3 of title 34, Code of Federal
22 Regulations, or any successor regulation;

23 (ix) political information or informa-
24 tion on criminal convictions or arrests;

1 (x) any required security code, access
2 code, password, or username necessary to
3 permit access to the account of an indi-
4 vidual;

5 (xi) characteristics of protected class-
6 es under Federal law, including race, color,
7 national origin, religion, sex, age, or dis-
8 ability; or

9 (xii) an inference drawn from any of
10 the information described in this subpara-
11 graph to create a profile about an indi-
12 vidual reflecting the individual's pref-
13 erences, characteristics, psychological
14 trends, preferences, predispositions, behav-
15 ior, attitudes, intelligence, abilities, or apti-
16 tudes.

17 (C) EXCLUSIONS.—

18 (i) IN GENERAL.—The term “personal
19 information” does not include publicly
20 available information.

21 (ii) PUBLICLY AVAILABLE INFORMA-
22 TION.—For purposes of clause (i), the
23 term “publicly available information”—

24 (I) means information that is
25 lawfully made available from Federal,

1 State, or local government records;
 2 and

3 (II) does not include—

4 (aa) biometric information
 5 collected by a covered entity
 6 about an individual without the
 7 individual's knowledge;

8 (bb) information used for a
 9 purpose that is not compatible
 10 with the purpose for which the
 11 information is maintained and
 12 made available in government
 13 records; or

14 (cc) information of an indi-
 15 vidual that is de-identified.

16 (11) THIRD PARTY.—The term “third party”,
 17 with respect to personal information of an indi-
 18 vidual, means any person that is not—

19 (A) the covered entity that is disclosing the
 20 personal information;

21 (B) solely performing an outsourced func-
 22 tion of the covered entity disclosing the personal
 23 information if—

24 (i) the person is contractually or le-
 25 gally prohibited from using, retaining,

1 sharing, or selling the personal information
 2 after the conclusion of the outsourced
 3 function; and

4 (ii) the person is complying with the
 5 regulations promulgated under this Act; or

6 (C) a person with respect to which the in-
 7 dividual gave specific opt-in approval for the
 8 covered entity to disclose the personal informa-
 9 tion of the individual to the person.

10 **SEC. 3. ACT PROHIBITED.**

11 (a) IN GENERAL.—It shall be unlawful for a covered
 12 entity to violate the privacy of an individual in a manner
 13 that violates a regulation promulgated under this Act.

14 (b) REGULATIONS.—In carrying out this Act, the
 15 Commission shall—

16 (1) not later than 1 year after the date of en-
 17 actment of this Act, promulgate regulations under
 18 section 553 of title 5, United States Code, to protect
 19 the individual and collective privacy rights set forth
 20 in this Act;

21 (2) ensure the regulations promulgated under
 22 paragraph (1) take effect not later than 90 days
 23 after the date on which the regulations are promul-
 24 gated;

1 (3) establish a centralized internet website for
 2 the benefit of individuals that provides information
 3 to individuals about their rights under this Act in a
 4 clear, concise, well-organized, understandably writ-
 5 ten, and complete manner; and

6 (4) establish a centralized internet website for
 7 the benefit of individuals that lists each data broker
 8 in the United States.

9 **SEC. 4. RIGHT TO NOTICE.**

10 (a) IN GENERAL.—In promulgating regulations
 11 under section 3, the Commission shall require a covered
 12 entity to—

13 (1) develop and make available to customers a
 14 short-form notice about the collection, retention, use,
 15 and sharing of the personal information of individ-
 16 uals by the covered entity that includes—

17 (A) what personal information is being col-
 18 lected, used, or retained;

19 (B) the manner in which the personal in-
 20 formation is collected;

21 (C) how and for what purpose the covered
 22 entity is collecting, using, retaining, sharing, or
 23 selling the personal information;

24 (D) how long the personal information will
 25 be held;

1 (E) which third parties the covered entity
2 shares personal information with or leases or
3 sells personal information to, not including—

4 (i) a governmental entity with which
5 the covered entity shares personal informa-
6 tion pursuant to a court order or law that
7 prohibits the covered entity from revealing
8 that instance of sharing to the individual
9 to whom the personal information pertains;

10 (ii) a third party if the personal infor-
11 mation is—

12 (I) made available to and readily
13 accessible by the general public with
14 the consent of the individual to whom
15 the personal information pertains; and

16 (II) shared with, or leased or sold
17 to, the third party through a mecha-
18 nism available to any member of the
19 general public; or

20 (iii) a third party with which the cov-
21 ered entity shares, or to which the covered
22 entity leases or sells, personal information
23 of an individual that the covered entity did
24 not obtain from the individual, if revealing
25 that instance of sharing, leasing, or selling

1 personal information would expose another
2 individual to likely harm;

3 (F) in the case of the sharing, leasing, or
4 selling of personal information described in sub-
5 paragraph (E) that is not excluded under clause
6 (i), (ii), or (iii) of that subparagraph, what per-
7 sonal information is shared with or leased or
8 sold to third parties and for what purpose;

9 (G) how an individual can access, correct,
10 and delete the personal information of the indi-
11 vidual that the covered entity retains as re-
12 quired under section 6;

13 (H) the practices of the covered entity for
14 collecting personal information of an individual,
15 including offline practices, when the individual
16 is not directly interacting with the covered enti-
17 ty;

18 (I) the practices of the covered entity for
19 using personal information in automated deci-
20 sionmaking; and

21 (J) the right of an individual to provide
22 opt-in approval and revoke approval consistent
23 with section 5;

24 (2) ensure that the short-form notice developed
25 under paragraph (1)—

1 (A) is clear, concise, well-organized, under-
2 standably written, and complete;

3 (B) does not contain unrelated, confusing,
4 or contradictory materials; and

5 (C) is in a format that is—

6 (i) prominent and easily accessible;

7 (ii) of reasonable length; and

8 (iii) clearly distinguishable from other
9 matters;

10 (3) not later than 15 days after making a mate-
11 rial change to the privacy practices or policies of the
12 covered entity, update the short-form notice devel-
13 oped under paragraph (1);

14 (4) make the short-form notice required under
15 paragraph (1) persistently and conspicuously avail-
16 able—

17 (A) on the website or mobile application of
18 the covered entity, if the covered entity main-
19 tains a website or mobile application; and

20 (B) at the physical place of business or
21 any other offline equivalent maintained by the
22 covered entity; and

23 (5) ensure that the short-form notice required
24 under paragraph (1) is made available to an indi-
25 vidual—

1 (A)(i) at the point of sale of a product or
 2 service of, subscription to a service of, or estab-
 3 lishment of an account with, the covered entity,
 4 prior to the sale, subscription, or establishment,
 5 whether that point of sale, subscription, or es-
 6 tablishment is in person, online, over the tele-
 7 phone, or through another means; or

8 (ii) if there is no such sale, subscription, or
 9 establishment, before the individual uses the
 10 product or service of the covered entity; and

11 (B) regardless of the decision of the indi-
 12 vidual as to whether to provide opt-in approval
 13 to the covered entity.

14 (b) REQUIREMENTS FOR UNEXPECTED COLLECTION
 15 OR USE OF PERSONAL INFORMATION.—

16 (1) IN GENERAL.—In promulgating regulations
 17 under section 3, the Commission shall apply the re-
 18 quirements under paragraph (2) of this subsection
 19 to any collection or use of personal information of an
 20 individual by a covered entity other than collection
 21 or use that—

22 (A) is necessary for the performance of a
 23 contract to which the individual is party;

1 (B) consists of actions that an individual
2 would consider necessary in order to provide a
3 requested product or service; or

4 (C) consists of actions taken at the request
5 of the individual prior to entering into a con-
6 tract to which the individual is party.

7 (2) REQUIREMENTS.—A covered entity that is
8 subject to paragraph (1), with respect to any indi-
9 vidual whose personal information the covered entity
10 collects or uses as described in that paragraph—

11 (A) shall provide the short-form notice de-
12 veloped under subsection (a)(1) to the indi-
13 vidual in a manner that ensures that the indi-
14 vidual reviews the notice and can provide opt-
15 in approval under section 5;

16 (B) shall notify the individual of any mate-
17 rial change to the privacy practices or policies
18 of the covered entity not later than the date on
19 which the covered entity updates the short-form
20 notice under subsection (a)(3);

21 (C) may not collect any personal informa-
22 tion of the individual not specified in the short-
23 form notice most recently provided to the indi-
24 vidual in accordance with subparagraph (A) un-
25 less the covered entity provides the individual

1 with a new short-form notice consistent with
2 that subparagraph at the point of collection of
3 the additional information; and

4 (D) may not use personal information of
5 the individual for a purpose not specified in the
6 short-form notice most recently provided to the
7 individual in accordance with subparagraph (A)
8 unless the covered entity provides the individual
9 with a new short-form notice consistent with
10 that paragraph that discloses the additional
11 purpose.

12 (c) STANDARDIZED SHORT-FORM PRIVACY NO-
13 TICE.—

14 (1) STANDARDIZED NOTICE.—The Commission
15 shall establish standardized short-form privacy no-
16 tices that comply with this section.

17 (2) USE OF STANDARDIZED NOTICE.—A cov-
18 ered entity may satisfy the requirements of sub-
19 section (a) by adopting a standardized short-form
20 privacy notice established by the Commission under
21 paragraph (1) of this subsection.

22 (d) JOINT NOTICE FOR AFFILIATED COVERED ENTI-
23 TIES.—Two or more affiliated covered entities may use a
24 single joint short-form notice for purposes of this section
25 if the short-form notice—

1 (1) states that the notice applies to multiple af-
2 filiated covered entities and names each such covered
3 entity; and

4 (2) is accurate with respect to the actions of
5 each covered entity using the notice.

6 **SEC. 5. RIGHT TO CONTROL.**

7 (a) **OPT-IN APPROVAL REQUIRED.**—In promulgating
8 regulations under section 3, the Commission shall require
9 a covered entity to obtain opt-in approval from an indi-
10 vidual to—

11 (1) collect, use, retain, share, or sell the individ-
12 ual’s personal information; or

13 (2) make any material changes in the collection,
14 use, retention, sharing, or sale of the individual’s
15 personal information.

16 (b) **RULES FOR APPROVAL.**—

17 (1) **PROCEDURES.**—A covered entity shall ob-
18 tain approval under subsection (a) in accordance
19 with the procedures for notification under section 4.

20 (2) **MANNER.**—In order to satisfy subsection
21 (a), approval shall be freely given, specific, informed,
22 and unambiguous.

23 (3) **WITHDRAWAL.**—An individual shall have
24 the right to withdraw his or her approval at any
25 time.

1 (4) MEANS.—A covered entity shall seek to ob-
2 tain approval through the primary medium used to
3 offer or deliver the covered entity’s product or serv-
4 ice.

5 (c) EXCEPTIONS.—A covered entity shall not be re-
6 quired to obtain opt-in approval from an individual under
7 subsection (a)—

8 (1) if collection is necessary for the perform-
9 ance of a contract to which the individual is party;

10 (2) to take steps that an individual would con-
11 sider necessary in order to provide a requested prod-
12 uct or service; or

13 (3) to take steps at the request of the individual
14 prior to entering into a contract to which the indi-
15 vidual is party.

16 (d) EMERGENCY OR EXIGENT CIRCUMSTANCES.—

17 (1) IN GENERAL.—Subject to paragraph (2), a
18 covered entity shall not be required to obtain opt-in
19 approval under subsection (a) if the covered entity,
20 in good faith, believes danger of death or serious
21 physical injury to any individual requires use, access,
22 or disclosure without delay of personal information
23 relating to the emergency.

24 (2) NOTICE REQUIREMENT.—Not later than 90
25 days after the date on which a covered entity uses,

1 accesses, or discloses personal information of an in-
 2 dividual without obtaining opt-in approval under
 3 paragraph (1), the covered entity shall inform the
 4 individual of—

5 (A) the personal information that the cov-
 6 ered entity used, accessed, or disclosed;

7 (B) the details of the emergency or exigent
 8 circumstances; and

9 (C) the reasons why the covered entity
 10 needed to use, access, or disclose the personal
 11 information.

12 (e) EXEMPTIONS.—

13 (1) IN GENERAL.—In promulgating regulations
 14 under subsection (a), the Commission may grant an
 15 exemption to a specific covered entity from the con-
 16 trol requirements under this section after taking into
 17 account—

18 (A) privacy risks posed by the use of per-
 19 sonal information by the covered entity;

20 (B) the costs and benefits of applying the
 21 regulations to the covered entity; and

22 (C) whether—

23 (i) the personal information held by
 24 the covered entity is—

1 (I) necessary and used, retained,
2 or shared only to protect the security
3 of the covered entity's service;

4 (II)(aa) necessary for providing a
5 service requested by an individual;
6 and

7 (bb) consistent with the context
8 of the service provided;

9 (III) necessary to initiate, render,
10 bill for, or collect payment for a serv-
11 ice or product requested by an indi-
12 vidual from the covered entity; or

13 (IV) necessary to protect—

14 (aa) the rights or property
15 of the covered entity; or

16 (bb) individuals who use the
17 services or products provided by
18 the covered entity or other cov-
19 ered entities from fraudulent,
20 abusive, or unlawful use of the
21 service or product; or

22 (ii) the covered entity—

23 (I) de-identifies the personal in-
24 formation held by the covered entity;
25 and

1 (II) where possible, provides indi-
 2 viduals with the choice to opt-out of
 3 the collection and use of the de-identi-
 4 fied information of the individuals.

5 (2) REPORTING REQUIREMENT.—If the Com-
 6 mission grants an exemption to a covered entity
 7 under paragraph (1), the Commission shall list the
 8 covered entity on the website of the Commission es-
 9 tablished under section 3(b)(3) and provide a brief
 10 justification for granting the exemption to the cov-
 11 ered entity.

12 **SEC. 6. RIGHT TO ACCESS, CORRECTION, DELETION, AND**
 13 **DATA PORTABILITY.**

14 (a) IN GENERAL.—In promulgating regulations
 15 under section 3, the Commission shall require a covered
 16 entity to—

17 (1) upon request, provide confirmation to an in-
 18 dividual who uses a product or service of the covered
 19 entity, or has established a subscription or account
 20 with the covered entity, as to whether the covered
 21 entity retains personal information pertaining to the
 22 individual;

23 (2) if the covered entity retains the individual's
 24 personal information, provide to the individual—

1 (A) reasonable means to access the per-
2 sonal information;

3 (B) a description of—

4 (i) the personal information being re-
5 tained;

6 (ii) each date on which the covered
7 entity collected the personal information;

8 (iii) the third parties to which the cov-
9 ered entity has disclosed or will disclose
10 the personal information; and

11 (iv) if possible, how long the personal
12 information will be retained or stored, or if
13 not possible, the criteria used for deter-
14 mining how long the personal information
15 will be retained or stored; and

16 (C) notice of the right to correct and delete
17 personal information;

18 (3) provide the access to the personal informa-
19 tion under paragraph (2)(A) in the form of a port-
20 able electronic table that—

21 (A) is in a usable and searchable format;

22 (B) allows the individual to transfer the
23 personal information from one entity to another
24 entity without hindrance; and

1 (C) to the extent that the Commission de-
2 termines practicable and appropriate, delineates
3 between—

4 (i) personal information collected and
5 shared in order to provide the individual
6 with the desired product or service; and

7 (ii) personal information that was sold
8 by the covered entity to a third party;

9 (4) provide an individual with a mechanism to
10 correct inaccurate personal information retained or
11 stored by the covered entity;

12 (5)(A) provide an individual with a mechanism
13 to request the deletion of the personal information
14 of the individual that the covered entity retains or
15 stores about the individual; and

16 (B) when the covered entity receives a request
17 from an individual under subparagraph (A), delete
18 the personal information collected from the indi-
19 vidual unless the covered entity needs to retain the
20 personal information in order to—

21 (i)(I) complete the transaction for which
22 the personal information was collected;

23 (II) provide a good or service requested by
24 the individual or reasonably anticipated within

1 the context of the covered entity's ongoing rela-
2 tionship with the individual; or

3 (III) otherwise perform a contract to which
4 the individual is party;

5 (ii) detect security incidents, protect
6 against activity that violates the covered enti-
7 ty's terms of service or malicious, deceptive,
8 fraudulent, or illegal activity, or prosecute per-
9 sons responsible for such activity;

10 (iii) debug to identify and repair errors
11 that impair existing functionality;

12 (iv) exercise free speech, ensure the ability
13 of another individual to exercise his or her right
14 to free speech, or exercise another right pro-
15 vided for by law;

16 (v) comply with chapter 119, 121, or 206
17 of title 18, United States Code;

18 (vi) engage in public or peer-reviewed sci-
19 entific, historical, or statistical research in the
20 public interest that adheres to all other applica-
21 ble ethics and privacy laws, if—

22 (I) the covered entity's deletion of the
23 information is likely to render impossible
24 or seriously impair the achievement of such
25 research;

1 (II) the individual has provided in-
2 formed consent; and

3 (III) the research is already in
4 progress at the time that deletion is re-
5 quested; or

6 (vii) comply with a legal obligation;

7 (6) provide the mechanisms under paragraphs
8 (4) and (5) in a form that is—

9 (A) clear and conspicuous; and

10 (B) made available—

11 (i) at no additional cost to the user;

12 (ii) without requiring an individual to
13 establish an account with the covered enti-
14 ty;

15 (iii) in a language other than English,
16 if the provider transacts business with in-
17 dividuals in that other language;

18 (iv) to individuals regardless of wheth-
19 er the information was obtained by the
20 covered entity directly from the individual,
21 not to include publicly available or de-iden-
22 tified personal information;

23 (v)(I) through a toll-free number;

24 (II) on the covered entity's website, if
25 the covered entity maintains a website; or

1 (III) through the primary mechanism
2 through which the covered entity engages
3 in a relationship with the individual in
4 order to provide a product or service; and

5 (vi) such that an individual has the
6 opportunity to request correction or dele-
7 tion of personal information not less fre-
8 quently than once every 6 months;

9 (7) inform any entity with which the covered
10 entity has shared, sold, or disclosed an individual's
11 personal information of any request from the indi-
12 vidual for confirmation of, access to, correction of,
13 or deletion of the individual's personal information
14 under this subsection;

15 (8) comply with an individual's request for con-
16 firmation, access, correction, or deletion under this
17 subsection even if the request is received from an-
18 other covered entity, if the receiving covered entity
19 can verify that the request is originally from the in-
20 dividual; and

21 (9) comply with an individual's request for con-
22 firmation, access, correction, or deletion under this
23 subsection not later than 90 days after receiving a
24 verifiable request from the individual or another cov-
25 ered entity.

1 (b) RIGHT OF PARENTS AND GUARDIANS OF MI-
 2 NORS.—For purposes of subsection (a), a parent or guard-
 3 ian of a minor may act on behalf of the minor with respect
 4 to personal information of the minor held by a covered
 5 entity, including by requesting confirmation of, access to,
 6 correction of, or deletion of the personal information.

7 (c) PROHIBITION ON DE-IDENTIFYING PERSONAL
 8 INFORMATION SUBSEQUENT TO REQUEST.—A covered
 9 entity may not de-identify an individual’s personal infor-
 10 mation during the 90-day period beginning on the date
 11 on which the covered entity receives a request from the
 12 individual for confirmation, access, correction, or deletion
 13 of the individual’s personal information under subsection
 14 (a).

15 **SEC. 7. PROHIBITION ON RE-IDENTIFYING PERSONAL IN-**
 16 **FORMATION.**

17 (a) IN GENERAL.—In promulgating regulations
 18 under section 3, the Commission shall require a covered
 19 entity to ensure that personal information that has been
 20 de-identified is not restored such that the information can
 21 be linked to a specific individual or device.

22 (b) ACTIONS REQUIRED.—In carrying out subsection
 23 (a), the Commission shall—

24 (1) require a covered entity to implement—

1 (A) technical safeguards that prohibit iden-
 2 tification of the individual to whom or device to
 3 which the information may pertain;

4 (B) processes that specifically prohibit re-
 5 identification of the information; and

6 (C) processes that prevent inadvertent re-
 7 lease of de-identified information; and

8 (2) prohibit a covered entity from making any
 9 attempt to reidentify the information.

10 **SEC. 8. PROHIBITION ON TAKE-IT-OR-LEAVE-IT.**

11 A covered entity may not refuse to serve an individual
 12 who does not approve the collection, use, retention, shar-
 13 ing, or sale of the individual’s personal information for
 14 commercial purposes on the basis of that lack of approval
 15 (commonly known as a “take-it-or-leave-it-offer”).

16 **SEC. 9. PROHIBITION ON FINANCIAL INCENTIVES.**

17 (a) IN GENERAL.—A covered entity may not offer an
 18 individual a program that relates the price of a product
 19 or service to the privacy protections afforded the indi-
 20 vidual, including by providing a discount or other incentive
 21 in exchange for the opt-in approval of the individual to
 22 the use and sharing of the individual’s personal informa-
 23 tion.

24 (b) RULE OF CONSTRUCTION.—Nothing in sub-
 25 section (a) shall be construed to prohibit the relation of

1 price of a service or the level of service provided to an
 2 individual to the provision, by the individual, of financial
 3 information that is necessarily collected and used only for
 4 the purpose of initiating, rendering, billing for, or col-
 5 lecting payment for a service or product requested by the
 6 individual from the covered entity.

7 (c) EXEMPTIONS.—The Commission may exempt a
 8 specific type of financial incentive offered by a particular
 9 covered entity from the prohibition under subsection (a)
 10 if the Commission determines that the type of financial
 11 incentive, as offered by that covered entity, is reasonable,
 12 just, and non-coercive.

13 **SEC. 10. PROHIBITION ON DISCLOSING INFORMATION TO**
 14 **THIRD PARTIES WITHOUT PROPER ASSUR-**
 15 **ANCES.**

16 (a) IN GENERAL.—A covered entity may not disclose
 17 the personal information of an individual to a third party
 18 under a written contract unless—

19 (1) the contract prohibits the third party
 20 from—

21 (A) using the personal information for any
 22 reason other than performing the specified serv-
 23 ice on behalf of the covered entity; or

24 (B) disclosing the personal information to
 25 another third party for any reason other than

1 performing the specified service on behalf of the
2 covered entity; and

3 (2) the covered entity ensures that the third
4 party effectively enforces the prohibitions described
5 in paragraph (1), including by auditing the data se-
6 curity and data information practices of the third
7 party not less frequently than once every 2 years.

8 (b) RULE OF CONSTRUCTION.—Nothing in sub-
9 section (a) shall be construed to prevent the disclosure of
10 personal information of an individual—

11 (1) by a covered entity to a third party if nec-
12 essary to comply with applicable law or a court-
13 issued subpoena, warrant, or order;

14 (2) by a covered entity to a third party that is
15 reasonably necessary to—

16 (A) address fraud, security, or technical
17 issues;

18 (B) protect the individual's rights or prop-
19 erty; or

20 (C) protect individuals or the public from
21 illegal activities as required or permitted by
22 law; or

23 (3) if the individual has specifically approved of
24 the disclosure.

1 **SEC. 11. USE LIMITATIONS.**

2 (a) IN GENERAL.—In promulgating regulations
3 under section 3, the Commission shall prohibit a covered
4 entity from using personal information for unreasonable
5 purposes, including—

6 (1) selling, leasing, trading, or otherwise prof-
7 iting from an individual's biometric information;

8 (2) sharing, resharing, or otherwise dissemi-
9 nating an individual's biometric information without
10 first obtaining specific consent from the individual,
11 unless—

12 (A) the dissemination is required by State
13 or Federal law or municipal ordinance; or

14 (B) the dissemination is required pursuant
15 to a valid warrant or subpoena issued by a
16 court of competent jurisdiction;

17 (3) processing personal information for the pur-
18 pose of advertising, marketing, soliciting, offering,
19 selling, leasing, licensing, renting, or otherwise com-
20 mercially contracting for employment, finance,
21 healthcare, credit, insurance, housing, or education
22 opportunities, in a manner that discriminates
23 against or otherwise makes the opportunity unavail-
24 able on the basis of a person's or class of persons'
25 actual or perceived race, color, ethnicity, religion,
26 national origin, sex, gender, gender identity, sexual

1 orientation, familial status, biometric information,
2 lawful source of income, or disability; or

3 (4) processing personal information in a man-
4 ner that segregates, discriminates in, or otherwise
5 makes unavailable the goods, services, facilities,
6 privileges, advantages, or accommodations of any
7 place of public accommodation on the basis of a per-
8 son's or class of persons' actual or perceived race,
9 color, ethnicity, religion, national origin, sex, gender,
10 gender identity, sexual orientation, or disability.

11 (b) DEFINITION OF PLACE OF PUBLIC ACCOMMODA-
12 TION.—For purposes of subsection (a), the term “place
13 of public accommodation” means—

14 (1) any entity considered a place of public ac-
15 commodation under section 201(b) of the Civil
16 Rights Act of 1964 (42 U.S.C. 2000a(b)) or section
17 301 of the Americans with Disabilities Act of 1990
18 (42 U.S.C. 12181); and

19 (2) any entity that offers goods or services
20 through the internet to the general public.

21 **SEC. 12. DATA MINIMIZATION.**

22 In promulgating regulations under section 3, the
23 Commission shall prohibit a covered entity from—

1 (1) collecting personal information of an indi-
2 vidual beyond what is adequate, relevant, and nec-
3 essary—

4 (A) for the performance of a contract to
5 which the individual is party;

6 (B) to provide a requested product or serv-
7 ice; or

8 (C) to take steps at the request of the indi-
9 vidual prior to entering into a contract to which
10 the individual is party; or

11 (2) accessing the personal information of an in-
12 dividual later than 90 days after the latest date on
13 which—

14 (A) the covered entity concludes the per-
15 formance of a contract to which the individual
16 is party;

17 (B) the covered entity concludes taking
18 steps that an individual would consider nec-
19 essary in order to provide a requested product
20 or service, including steps to prevent fraud, en-
21 sure safety, or ensure compliance with the cov-
22 ered entity's terms of service; or

23 (C) the individual otherwise terminates his
24 or her relationship with the covered entity.

1 **SEC. 13. RIGHT TO DATA SECURITY.**

2 (a) REASONABLE PROCEDURES.—

3 (1) IN GENERAL.—In promulgating regulations
4 under section 3, the Commission shall require a cov-
5 ered entity to establish and maintain reasonable
6 data security practices to protect the confidentiality,
7 integrity, and availability of personal information.

8 (2) PROPORTIONALITY.—The requirements pre-
9 scribed under paragraph (1) shall provide for secu-
10 rity procedures that are proportional to the volume
11 and nature of the personal information a covered en-
12 tity collects.

13 (3) COMMISSION GUIDANCE; INDUSTRY PRAC-
14 TICES.—The requirements prescribed under para-
15 graph (1) shall be consistent with guidance provided
16 by the Commission and recognized industry practices
17 for safety and security, including administrative,
18 technical, and physical safeguards to secure the per-
19 sonal information of users.

20 (4) TECHNOLOGICALLY NEUTRAL.—The Com-
21 mission may not require a specific technological
22 means of meeting a requirement under paragraph
23 (1).

24 (b) OTHER REQUIREMENTS.—In promulgating regu-
25 lations under section 3, the Commission shall require a
26 covered entity—

1 (1) to make publicly available a description of
2 the practices established by the covered entity under
3 subsection (a) that details—

4 (A) how the covered entity will address pri-
5 vacy and security risks associated with the de-
6 velopment of new products and services;

7 (B) the access that employees and contrac-
8 tors of the covered entity have to the personal
9 information of an individual who uses a service
10 or product of the covered entity; and

11 (C) the internal policies of the covered en-
12 tity for the use of the personal information de-
13 scribed in subparagraph (B);

14 (2)(A) to notify an individual if the covered en-
15 tity determines that—

16 (i) an unauthorized disclosure of the per-
17 sonal information of the individual has oc-
18 curred; and

19 (ii) harm is reasonably likely to occur; and

20 (B) as part of the notification under subpara-
21 graph (A), to offer the individual—

22 (i) the option to prohibit the covered entity
23 from collecting, using, retaining, sharing, or
24 selling the personal information of the indi-
25 vidual; and

1 (ii) the option to have the covered entity—

2 (I) erase all personal information of
3 the individual held by the covered entity;

4 (II) cease sharing and selling the per-
5 sonal information of the individual;

6 (III) provide the individual a copy of
7 the personal information of the individual
8 that the covered entity holds about the in-
9 dividual in a format consistent with section
10 6(a)(3); or

11 (IV) close the individual's account or
12 otherwise terminate the individual's rela-
13 tionship with the covered entity; and

14 (3) not less frequently than once every 2
15 years—

16 (A) to audit the privacy and security prac-
17 tices in place that protect the confidentiality,
18 integrity, and availability of personal informa-
19 tion held by the covered entity; or

20 (B) if the Commission determines it appro-
21 priate based on the volume and nature of the
22 personal information collected by the covered
23 entity, to—

- 1 (i) have an independent third-party
2 auditor conduct the audit described in sub-
3 paragraph (A); and
4 (ii) make the results of the audit
5 available to the Commission upon comple-
6 tion.

7 **SEC. 14. PRIVACY AND SECURITY OFFICER.**

8 In promulgating regulations under section 3, the
9 Commission shall require a covered entity to—

- 10 (1) designate not less than 1 employee of the
11 covered entity to coordinate the efforts to comply
12 with and carry out the responsibilities of the covered
13 entity under this Act, including any request or chal-
14 lenge related to personal information; and
15 (2) provide publicly accessible contact informa-
16 tion for each employee designated under paragraph
17 (1).

18 **SEC. 15. FEDERAL ENFORCEMENT.**

19 (a) ENFORCEMENT BY THE COMMISSION.—

- 20 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
21 TICES.—Except as provided in subsection (b), a vio-
22 lation of this Act or a regulation promulgated under
23 this Act shall be treated as a violation of a rule de-
24 fining an unfair or deceptive act or practice pre-

scribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) POWERS OF THE COMMISSION.—

(A) IN GENERAL.—Except as provided in subsection (b), the Commission shall enforce this Act and any regulations promulgated under this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act.

(B) PRIVILEGES AND IMMUNITIES.—Any person who violates this Act or a regulation promulgated under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(b) ENTITIES NOT REGULATED BY THE COMMISSION.—Compliance with this Act and the regulations promulgated under this Act shall be enforced as follows:

(1) Under section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818) by the appropriate Federal banking agency, with respect to an insured

1 depository institution (as those terms are defined in
2 section 3 of that Act (12 U.S.C. 1813)).

3 (2) Under the Federal Credit Union Act (12
4 U.S.C. 1751 et seq.) by the National Credit Union
5 Administration Board, with respect to any Federal
6 credit union.

7 (3) Under part A of subtitle VII of title 49,
8 United States Code, by the Secretary of Transpor-
9 tation, with respect to any air carrier or foreign air
10 carrier subject to that part.

11 (4) Under the Packers and Stockyards Act,
12 1921 (7 U.S.C. 181 et seq.) (except as provided in
13 section 406 of that Act (7 U.S.C. 226, 227)) by the
14 Secretary of Agriculture, with respect to any activi-
15 ties subject to that Act.

16 (5) Under the Farm Credit Act of 1971 (12
17 U.S.C. 2001 et seq.) by the Farm Credit Adminis-
18 tration, with respect to any Federal land bank, Fed-
19 eral land bank association, Federal intermediate
20 credit bank, or production credit association.

21 (c) RELATION TO PRIVATE AGREEMENTS.—It shall
22 be unlawful for any covered entity to commit an act pro-
23 hibited under this Act or a regulation promulgated under
24 this Act, regardless of any specific agreement between en-
25 tities or individuals.

1 (d) NO WAIVER OF RIGHTS AND REMEDIES.—The
 2 rights and remedies provided under this Act may not be
 3 waived or limited by contract or otherwise.

4 **SEC. 16. STATE ENFORCEMENT.**

5 (a) IN GENERAL.—In any case in which the attorney
 6 general of a State has reason to believe that an interest
 7 of the residents of that State has been or is threatened
 8 or adversely affected by the engagement of any covered
 9 entity in a practice that violates this Act or a regulation
 10 promulgated under this Act, the attorney general of the
 11 State may, as *parens patriae*, bring a civil action on behalf
 12 of the residents of the State in an appropriate district
 13 court of the United States to—

14 (1) enjoin that practice;

15 (2) enforce compliance with this Act or the reg-
 16 ulation;

17 (3) obtain damages, restitution, or other com-
 18 pensation on behalf of residents of the State; or

19 (4) obtain any other relief that the court con-
 20 sider appropriate.

21 (b) NOTICE.—

22 (1) IN GENERAL.—Before filing an action
 23 under subsection (a), the attorney general of the
 24 State involved shall provide to the Commission—

25 (A) written notice of the action; and

1 (B) a copy of the complaint for the action.

2 (2) EXEMPTION.—

3 (A) IN GENERAL.—Paragraph (1) shall not
4 apply with respect to the filing of an action by
5 an attorney general of a State if the attorney
6 general determines that it is not feasible to pro-
7 vide the notice described in that paragraph be-
8 fore the filing of the action.

9 (B) NOTIFICATION.—In an action de-
10 scribed in subparagraph (A), the attorney gen-
11 eral of a State shall provide notice and a copy
12 of the complaint to the Commission at the same
13 time as the attorney general files the action.

14 (c) INTERVENTION.—

15 (1) IN GENERAL.—Upon receiving notice under
16 subsection (b), the Commission shall have the right
17 to intervene in the action that is the subject of the
18 notice.

19 (2) EFFECT.—If the Commission intervenes in
20 an action under paragraph (1), the Commission shall
21 have the right—

22 (A) to be heard with respect to any matter
23 that arises in the action; and

24 (B) to file a petition for appeal.

1 (d) RULE OF CONSTRUCTION.—For purposes of
 2 bringing a civil action under subsection (a), nothing in this
 3 Act shall be construed to prevent the attorney general of
 4 a State from exercising the powers conferred on the attor-
 5 ney general by the laws of the State to—

6 (1) conduct investigations;

7 (2) administer oaths or affirmations; or

8 (3) compel the attendance of witnesses or the
 9 production of documentary and other evidence.

10 (e) PREEMPTIVE ACTION BY COMMISSION.—If the
 11 Commission institutes an action with respect to a violation
 12 of this Act or a regulation promulgated under this Act,
 13 a State may not, during the pendency of that action, insti-
 14 tute an action under subsection (a) against any defendant
 15 named in the complaint in the action instituted by the
 16 Commission based on the same set of facts giving rise to
 17 the violation with respect to which the Commission insti-
 18 tuted the action.

19 **SEC. 17. PRIVATE RIGHT OF ACTION.**

20 (a) RIGHT OF ACTION.—

21 (1) IN GENERAL.—Any individual alleging a
 22 violation of this Act or a regulation promulgated
 23 under this Act may bring a civil action in any court
 24 of competent jurisdiction.

1 (2) INJURY IN FACT.—A violation of this Act or
2 a regulation promulgated under this Act with re-
3 spect to the personal information of an individual
4 constitutes an injury in fact to that individual.

5 (b) RELIEF.—In a civil action brought under sub-
6 section (a) in which the plaintiff prevails, the court may
7 award—

- 8 (1) actual damages;
- 9 (2) punitive damages;
- 10 (3) reasonable attorney’s fees and costs; and
- 11 (4) any other relief, including an injunction,
- 12 that the court determines appropriate.

13 (c) PRE-DISPUTE ARBITRATION AGREEMENTS.—

14 (1) IN GENERAL.—Notwithstanding any other
15 provision of law, no pre-dispute arbitration agree-
16 ment shall be valid or enforceable with respect to a
17 dispute between a covered entity and an individual
18 that relates to a violation of this Act or a regulation
19 promulgated under this Act.

20 (2) APPLICABILITY.—An issue as to whether
21 this subsection applies with respect to a dispute
22 shall be determined by a court. The validity and en-
23 forceability of an agreement to which this subsection
24 applies shall be determined by a court, rather than
25 an arbitrator, irrespective of whether the agreement

1 purports to delegate such determinations to an arbi-
2 trator.

3 **SEC. 18. RELATION TO OTHER LAWS.**

4 (a) IN GENERAL.—Except as provided in subsection
5 (b), nothing in this Act shall be construed to—

6 (1) modify, limit, or supersede the operation of
7 any privacy or security provision in—

8 (A) section 552a of title 5, United States
9 Code (commonly known as the “Privacy Act of
10 1974”);

11 (B) the Right to Financial Privacy Act of
12 1978 (12 U.S.C. 3401 et seq.);

13 (C) the Fair Credit Reporting Act (15
14 U.S.C. 1681 et seq.);

15 (D) the Fair Debt Collection Practices Act
16 (15 U.S.C. 1692 et seq.);

17 (E) the Children’s Online Privacy Protec-
18 tion Act of 1998 (15 U.S.C. 6501 et seq.);

19 (F) title V of the Gramm-Leach-Bliley Act
20 (15 U.S.C. 6801 et seq.);

21 (G) chapters 119, 123, and 206 of title 18,
22 United States Code;

23 (H) section 444 of the General Education
24 Provisions Act (20 U.S.C. 1232g) (commonly

1 referred to as the “Family Educational Rights
2 and Privacy Act of 1974”);

3 (I) section 445 of the General Education
4 Provisions Act (20 U.S.C. 1232h);

5 (J) the Privacy Protection Act of 1980 (42
6 U.S.C. 2000aa et seq.);

7 (K) the regulations promulgated under sec-
8 tion 264(c) of the Health Insurance Portability
9 and Accountability Act of 1996 (42 U.S.C.
10 1320d–2 note), as those regulations relate to—

11 (i) a person described in section
12 1172(a) of the Social Security Act (42
13 U.S.C. 1320d–1(a)); or

14 (ii) transactions referred to in section
15 1173(a)(1) of the Social Security Act (42
16 U.S.C. 1320d–2(a)(1));

17 (L) the Communications Assistance for
18 Law Enforcement Act (47 U.S.C. 1001 et seq.);

19 (M) sections 222 and 227 of the Commu-
20 nications Act of 1934 (47 U.S.C. 222, 227); or

21 (N) any other privacy or security provision
22 of Federal law;

23 (2) limit the authority of the Commission under
24 any other provision of law; or

1 (3) limit the authority of the Federal Commu-
2 nications Commission to promulgate regulations and
3 enforce any privacy law not in contradiction with
4 this Act.

5 (b) APPLICABILITY TO MINORS.—To the extent that
6 a provision of this Act or a regulation promulgated under
7 this Act is inconsistent with a provision of any other Fed-
8 eral law relating to the protection and control of the per-
9 sonal information of minors, the provision that provides
10 the most protection and control to minors and their par-
11 ents or guardians shall apply.

12 **SEC. 19. EFFECTIVE DATE.**

13 This Act shall take effect on the date that is 90 days
14 after the date of enactment of this Act.

○