

117TH CONGRESS
1ST SESSION

S. 1494

To protect the privacy of consumers.

IN THE SENATE OF THE UNITED STATES

APRIL 29, 2021

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

A BILL

To protect the privacy of consumers.

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 “Consumer Data Privacy and Security Act of 2021”.

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

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

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

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) BIOMETRIC INFORMATION.—The term “bio-
 4 metric information” means information, resulting
 5 from specific technical processing related to the
 6 physical, biological, physiological, genetic, or behav-
 7 ioral characteristics of an individual, that identifies
 8 the individual.

9 (2) COLLECTION.—The term “collection”
 10 means acquiring personal data by any means, in-
 11 cluding by receiving, purchasing, or leasing the data
 12 or by observing or interacting with the individual to
 13 whom the data relates.

14 (3) COMMISSION.—The term “Commission”
 15 means the Federal Trade Commission.

16 (4) COVERED ENTITY.—

17 (A) IN GENERAL.—The term “covered en-
 18 tity” means any entity that—

19 (i) alone, or jointly with others, deter-
 20 mines the purpose and means of collecting
 21 or processing personal data; and

22 (ii) is—

1 (I) a person over which the Com-
2 mission has authority pursuant to sec-
3 tion 5(a)(2) of the Federal Trade
4 Commission Act (15 U.S.C. 45(a)(2));

5 (II) a common carrier subject to
6 the Communications Act of 1934 (47
7 U.S.C. 151 et seq.) and Acts amend-
8 atory thereof and supplementary
9 thereto; or

10 (III) a nonprofit organization, in-
11 cluding any organization that is not
12 organized to carry on business for its
13 own profit or that of its members.

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

18 (5) DE-IDENTIFY.—The term “de-identify”
19 means, with respect to personal data held by a cov-
20 ered entity or service provider, that the covered enti-
21 ty or service provider—

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

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

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

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

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

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

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

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

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

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

(9) PERSONAL DATA.—

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

(B) LINKED OR REASONABLY LINKABLE.—

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

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

1 is used to identify a specific individual over
2 time and across services and platforms, in-
3 cluding a customer number held in a cook-
4 ie, a static Internet Protocol (IP) address,
5 a processor or device serial number, or an-
6 other unique device identifier, shall be con-
7 sidered information that is linked or rea-
8 sonably linkable to the individual for pur-
9 poses of subparagraph (A).

10 (C) EXCLUSION.—The term “personal
11 data” does not include—

- 12 (i) de-identified data;
- 13 (ii) data that has been rendered
14 unreadable or indecipherable;
- 15 (iii) information about employees or
16 employment status collected or used by an
17 employer pursuant to an employer-em-
18 ployee relationship, including information
19 related to prospective employees and rel-
20 evant application materials;
- 21 (iv) publicly available information;
- 22 (v) data that has undergone
23 pseudonymization; or
- 24 (vi) employee data.

1 (D) EMPLOYEE DATA.—For purposes of
2 subparagraph (C), the term “employee data”
3 means information collected by a covered entity
4 or the service provider of a covered entity that
5 is—

6 (i) contact information for an indi-
7 vidual or the individual’s emergency con-
8 tact that is collected in the course of the
9 individual’s employment or application for
10 employment (including on a contract or
11 temporary basis) with the covered entity,
12 provided that such information is retained
13 or processed by the covered entity or serv-
14 ice provider solely for purposes related to
15 the individual’s employment or application
16 for employment with the covered entity; or

17 (ii) information about an individual
18 who is an employee or former employee of
19 the covered entity (or a relative of such an
20 individual) that is necessary to administer
21 benefits to which such individual or rel-
22 ative is entitled on the basis of the individ-
23 ual’s employment with the covered entity,
24 provided that such data is retained or
25 processed by the covered entity or service

1 provider solely for the purpose of admin-
2 istering such benefits.

3 (10) PSEUDONYMIZATION.—The term “pseudo-
4 nymization” means the processing of personal data
5 so that the personal data can no longer be attributed
6 or reasonably linked to a specific individual without
7 the use of additional information, provided that such
8 additional information—

9 (A) is kept separately; and

10 (B) is subject to technical and organiza-
11 tional measures to ensure that the personal
12 data is not attributed to a specific individual.

13 (11) PRIVACY OFFICER.—The term “privacy of-
14 ficer” means an individual designated by a covered
15 entity or service provider under section 7(b)(1) to be
16 the privacy officer of the covered entity.

17 (12) PROCESSING.—The term “processing”
18 means any operation or set of operations performed
19 on personal data, including the analysis, organiza-
20 tion, structuring, retaining, using, disclosing, trans-
21 mitting, sharing, transferring, selling, licensing, or
22 otherwise handling of personal data.

23 (13) PUBLICLY AVAILABLE INFORMATION.—

24 (A) IN GENERAL.—The term “publicly
25 available information” means any information

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

4 (i) a Federal, State, or local govern-
5 ment record;

6 (ii) widely distributed media; or

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

11 (B) REASONABLE BASIS TO BELIEVE.—

12 For purposes of subparagraph (A), reasonable
13 bases for believing that information is lawfully
14 made available to the general public shall in-
15 clude a written determination by a covered enti-
16 ty or service provider that the information is of
17 a type that is lawfully made available to the
18 general public.

19 (14) SENSITIVE PERSONAL DATA.—The term
20 “sensitive personal data” means personal data that
21 is—

22 (A) a unique, government-issued identifier,
23 such as a social security number, passport num-
24 ber, driver’s license number, or taxpayer identi-
25 fication number;

1 (B) a user name or email address in com-
2 bination with a password or security question
3 and answer that would permit access to an on-
4 line account;

5 (C) biometric information of an individual;

6 (D) the content of a wire communication,
7 oral communication, or electronic communica-
8 tion, as those terms are defined in section 2510
9 of title 18, United States Code, to which the in-
10 dividual is a party, unless the covered entity is
11 the intended recipient of the communication;

12 (E) information that relates to—

13 (i) the past, present, or future diag-
14 nosed physical or mental health or condi-
15 tion of an individual;

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

18 (iii) the past, present, or future pay-
19 ment for the provision of health care to an
20 individual;

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

25 (G) the race or ethnicity of the individual;

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

3 (I) the sexual orientation of the individual;

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

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

16 (15) SERVICE PROVIDER.—The term “service
17 provider” means an entity that collects or processes
18 personal data on behalf of, and at the direction of,
19 a covered entity to which the service provider is un-
20 affiliated, but only—

21 (A) with respect to the personal data col-
22 lected or processed on the behalf of, and at the
23 direction of, such covered entity; and

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

1 (i) is on the behalf of, and at the di-
2 rection of, such covered entity; or

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

4 (16) SMALL BUSINESS.—The term “small busi-
5 ness” means any covered entity or service provider
6 that—

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

8 (i) employs not more than 500 em-
9 ployees; and

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

13 (B) collects or processes on an annual
14 basis—

15 (i) the personal data of fewer than
16 1,000,000 individuals; or

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

19 (17) THIRD PARTY.—

20 (A) IN GENERAL.—The term “third party”
21 means a covered entity that receives third party
22 personal data from an unaffiliated covered enti-
23 ty, but only with respect to such third party
24 personal data.

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

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

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

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

SEC. 3. COLLECTION AND PROCESSING OF PERSONAL DATA.

(a) REQUIREMENTS.—

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

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

1 (B) the covered entity collects or processes
2 the personal data in accordance with a permis-
3 sible purpose described in subsection (c).

4 (2) APPLICATION TO THIRD PARTIES.—

5 (A) IN GENERAL.—A covered entity that is
6 a third party with respect to the personal data
7 of an individual may collect or process such per-
8 sonal data without directly obtaining the indi-
9 vidual's consent as required under paragraph
10 (1)(A) if—

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

14 (I) has provided the individual
15 with notice of—

16 (aa) the fact that the cov-
17 ered entity would disclose the in-
18 dividual's personal data to the
19 third party; and

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

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

1 or processing of the individual's per-
 2 sonal data; or

3 (ii) the third party collects or process
 4 the personal data in accordance with a per-
 5 missible purpose described in subsection
 6 (c).

7 (B) NOTICE AND CONSENT REQUIREMENT
 8 FOR DIFFERENT OR ADDITIONAL COLLECTION
 9 OR PROCESSING.—A covered entity that is a
 10 third party with respect to the personal data of
 11 an individual shall obtain the consent of such
 12 individual in accordance with subsection (b) be-
 13 fore collecting or processing such personal data
 14 if the specific purpose for such collection or
 15 processing—

16 (i) is not a purpose described in para-
 17 graph (1), (2), (4), or (6) of subsection (c);
 18 and

19 (ii) is different from, or in addition to,
 20 the purpose for any collection or processing
 21 to which the individual previously con-
 22 sented in accordance with subsection (b).

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

1 subparagraph (A), a covered entity that is a
2 third party with respect to the personal data of
3 an individual may reasonably rely on represen-
4 tations made by the covered entity from whom
5 the third party received such data regarding the
6 notice provided to, and the consent obtained
7 from, such individual, provided that the third
8 party has determined, after exercising reason-
9 able due diligence, that the covered entity is
10 credible.

11 (3) NOTICE AND CONSENT OBTAINED BY SERV-
12 ICE PROVIDERS.—A service provider may provide no-
13 tice to, and obtain consent from, an individual in ac-
14 cordance with subsection (b) on behalf of a covered
15 entity.

16 (b) CONSENT.—

17 (1) IN GENERAL.—

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

1 (B) EXPRESS AFFIRMATIVE CONSENT RE-
 2 QUIREMENT.—

3 (i) IN GENERAL.—The express affirm-
 4 ative consent of an individual is required to
 5 collect or process the personal data of the
 6 individual if the collection or processing—

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

9 (II) involves the disclosure of
 10 personal data to a third party for a
 11 purpose that is not described in sub-
 12 section (c).

13 (ii) REQUIREMENTS FOR VALID EX-
 14 PRESS AFFIRMATIVE CONSENT.—For pur-
 15 poses of clause (i), the express affirmative
 16 consent of an individual to a request to
 17 collect or process the personal data of the
 18 individual—

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

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

24 (III) cannot be inferred from in-
 25 action.

1 (2) NOTICE REQUIRED.—

2 (A) IN GENERAL.—In requesting the con-
3 sent of an individual to collect or process the
4 individual's personal data, a covered entity shall
5 provide the individual with notice, in a concise,
6 meaningful, timely, prominent, and easy-to-un-
7 derstand format, that includes—

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

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

13 (iii) the information described in sub-
14 paragraph (B).

15 (B) CONTENTS.—The notice provided by a
16 covered entity under subparagraph (A) shall in-
17 clude—

18 (i) information on how the individual
19 may access the privacy policy of the cov-
20 ered entity described in section 4(a);

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

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

1 (I) includes the disclosure of per-
2 sonal data to third parties; or

3 (II) involves sensitive personal
4 data.

5 (C) SEPARATION.—If consent is obtained
6 in the context of a notice that also concerns
7 matters other than the collection or processing
8 of personal data, the request for consent shall
9 be presented in a manner that is clearly distin-
10 guishable from the other matters.

11 (3) WITHDRAWAL OF CONSENT.—

12 (A) IN GENERAL.—A covered entity shall
13 provide an individual with the means to with-
14 draw previously given consent to collect or proc-
15 ess the personal data of the individual—

16 (i) at any time and place that is rea-
17 sonably practicable; and

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

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

22 (i) shall take effect without undue
23 delay;

1 (ii) shall remain in effect until the in-
 2 dividual revokes or limits that denial or
 3 withdrawal; and

4 (iii) shall not apply to any collection
 5 or processing of personal data that oc-
 6 curred before the date on which the with-
 7 drawal is made.

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

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

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

21 (B) take steps in furtherance of the re-
 22 quest initiated by the individual prior to pro-
 23 viding the service or entering into a contract or
 24 transaction.

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

7 (3) IMMEDIATE DANGER.—To prevent immi-
 8 nent danger to the personal safety of any individual,
 9 including by effectuating a product recall pursuant
 10 to Federal or State law.

11 (4) FRAUD PREVENTION AND PROTECTION OF
 12 SECURITY.—To protect the rights, property, services,
 13 or information systems of the covered entity or serv-
 14 ice provider, or any individual, including to inves-
 15 tigate a possible crime or to protect against security
 16 threats, abuse, malicious conduct, deception, fraud,
 17 theft, unauthorized transactions, or any other unlaw-
 18 ful activity.

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

21 (A) is performed for the primary purpose
 22 of advancing a broadly recognized public inter-
 23 est;

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

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

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

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

(6) OPERATIONAL PURPOSES.—To—

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

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

(i) is not disclosed to a third party;

and

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

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

1 from the individual by the covered entity or by
2 a service provider on behalf of the covered enti-
3 ty;

4 (D) improve a product, service, or activity
5 used, requested, or authorized by the individual,
6 including analytics, forecasting, the repair of er-
7 rors that impair existing intended functionality,
8 actions to verify or maintain quality or safety of
9 the product, service, or activity, or the ongoing
10 provision of customer service and support by
11 the covered entity or service provider; or

12 (E) other additional specific categories of
13 operational purposes that the Commission may
14 define by rule, issued in accordance with section
15 553 of title 5, United States Code.

16 (d) LIMITING THE RETENTION OF SENSITIVE PER-
17 SONAL DATA.—A covered entity shall delete or de-identify
18 sensitive personal data, and shall direct its service pro-
19 viders to delete or de-identify sensitive personal data, after
20 the data is no longer reasonably necessary to accomplish
21 the intended purposes permitted by this section, unless
22 such deletion or de-identification is impossible or demon-
23 strably impracticable.

24 (e) BANKRUPTCY.—If a covered entity or service pro-
25 vider commences a case under title 11 of the United States

1 Code, and the case or any proceeding under the case is
2 expected to lead to the disclosure of the personal data of
3 any individual, the covered entity or service provider shall,
4 in a reasonable amount of time before the disclosure, pro-
5 vide each individual whose personal data is subject to the
6 disclosure with—

7 (1) a notice of the proposed disclosure, includ-
8 ing—

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

11 (B) a description of the policies and prac-
12 tices relating to personal data of each such
13 third party; and

14 (2) the opportunity to—

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

18 (B) request that the covered entity or serv-
19 ice provider delete or de-identify the personal
20 data.

21 **SEC. 4. RIGHT TO KNOW.**

22 (a) IN GENERAL.—A covered entity shall make pub-
23 licly available, in a clear and prominent location and in
24 easy-to-understand language, a privacy policy that in-
25 cludes—

1 (1) a clear and specific description of the enti-
 2 ty's policies and practices with respect to personal
 3 data;

4 (2) a clear and specific description of the rights
 5 of individuals with respect to their personal data (in-
 6 cluding the rights described in section 5) and infor-
 7 mation on how to exercise those rights; and

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

9 (b) AVAILABILITY OF PREVIOUS VERSIONS.—A cov-
 10 ered entity shall make publicly available any previous
 11 version of a privacy policy required under subsection (a).

12 (c) CONTENTS.—A privacy policy required under sub-
 13 section (a) shall include—

14 (1) the identity and the contact details of the
 15 covered entity, including, where applicable, the rep-
 16 resentative of the covered entity for purposes of pri-
 17 vacy inquiries or its privacy officer;

18 (2) a clear description of each category of per-
 19 sonal data collected by the covered entity and the
 20 purposes for which each such category is collected
 21 and processed;

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

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

3 (4) whether, and for what purposes, the covered
4 entity discloses personal data to third parties, each
5 category of personal data disclosed to third parties,
6 and the types of third parties to which those cat-
7 egories of personal data are disclosed;

8 (5) whether, and for what purposes, the covered
9 entity receives personal data from third parties, the
10 categories of personal data received from third par-
11 ties, and the types of third parties from which the
12 covered entity receives personal data;

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

17 (7) the specific steps an individual may take to
18 minimize the collection or processing by the covered
19 entity of the individual's personal data, and the rel-
20 evant implications to the individual from minimizing
21 such collection or processing; and

22 (8) the effective date of the privacy policy.

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

1 section with respect to the collection or processing of per-
2 sonal data that is reasonably necessary and limited to—

3 (1) an in-person transaction where the personal
4 data is not processed for further purposes incompat-
5 ible with that transaction;

6 (2) comply a Federal, State, or local law or an-
7 other applicable legal requirement, including a sub-
8 poena, summons, or other properly executed compul-
9 sory process;

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

12 (4) protect the rights or data security of the
13 covered entity, a service provider of the covered enti-
14 ty, or any individual, including to investigate a pos-
15 sible crime or to protect against security threats,
16 abuse, fraud, theft, unauthorized transactions, or
17 any other unlawful activity.

18 (e) MATERIAL CHANGES.—

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

24 (A) shall notify each individual whose per-
25 sonal data is collected or processed by the cov-

1 ered entity, or a service provider on behalf of
2 the covered entity, with a description of the ma-
3 terial change, including—

4 (i) change to the categories of per-
5 sonal data the covered entity or service
6 provider processes;

7 (ii) change to the purposes for which
8 the covered entity or service provider proc-
9 esses personal data;

10 (iii) change to the manner in which
11 the covered entity or service provider dis-
12 closes personal data to third parties; and

13 (iv) which, if any, changes are retro-
14 active; and

15 (B) shall not process (or, in the case of a
16 material change to the privacy policy of a serv-
17 ice provider that is directed by the covered enti-
18 ty, shall not direct the service provider to proc-
19 ess) any sensitive personal data of an individual
20 that was collected by the covered entity or serv-
21 ice provider before the effective date of the ma-
22 terial change in a manner that is inconsistent
23 with the privacy policy that was applicable at
24 the time such data was collected until the indi-

1 vidual provides express affirmative consent to
2 such processing.

3 (2) DIRECT NOTICE OF MATERIAL CHANGE TO
4 AFFECTED INDIVIDUALS.—A covered entity shall, if
5 operationally and technically feasible, directly pro-
6 vide the notice of a material change required under
7 paragraph (1)(A) to each affected individual, taking
8 into account available technology and the nature of
9 the relationship between the covered entity and the
10 individual.

11 (3) PUBLIC NOTICE OF MATERIAL CHANGE.—
12 Where directly providing the notice of a material
13 change required under paragraph (1)(A) to each af-
14 fected individual is impossible or demonstrably im-
15 practicable, a covered entity—

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

18 (B) shall not process personal data that
19 was collected by the covered entity before the
20 effective date of the material change in a man-
21 ner that is inconsistent with the privacy policy
22 that was applicable at the time such data was
23 collected until after the notice has been so pub-
24 lished for a period of time that is reasonably
25 sufficient to give affected individuals the oppor-

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

3 **SEC. 5. INDIVIDUAL CONTROL.**

4 (a) **PRIVACY CONTROLS.**—Each covered entity
5 shall—

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

12 (2) if applicable, offer the means required
13 under paragraph (1) through the same means that
14 the individual routinely uses to interact with the cov-
15 ered entity; and

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

18 (b) **RIGHT TO ACCESS.**—

19 (1) **IN GENERAL.**—A covered entity shall, in re-
20 sponse to a verified request from an individual—

21 (A) confirm whether or not the covered en-
22 tity has collected or processed the personal data
23 of the individual; and

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

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

3 (i) a copy, or an accurate representa-
4 tion, of the personal data pertaining to the
5 individual collected and processed by the
6 covered entity; and

7 (ii) a list of the categories of third
8 parties to which the covered entity has dis-
9 closed the personal data of the individual,
10 if applicable.

11 (2) EASE OF ACCESS.—

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

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

17 (ii) providing the information elec-
18 tronically is impossible or demonstrably
19 impracticable.

20 (B) DATA PORTABILITY.—If a covered en-
21 tity provides an individual with information in
22 an electronic format under subparagraph (A),
23 the covered entity shall, where technically fea-
24 sible and reasonably practicable, provide the in-
25 dividual with—

1 (i) the ability to export the personal
2 data generated and submitted by the indi-
3 vidual in a structured, commonly-used, and
4 machine-readable format; and

5 (ii) the ability to transmit such infor-
6 mation to another entity without con-
7 straints or conditions.

8 (c) RIGHTS TO ACCURACY AND CORRECTION.—

9 (1) IN GENERAL.—A covered entity shall estab-
10 lish reasonable procedures designed to—

11 (A) ensure that the personal data that the
12 covered entity collects and processes with re-
13 spect to an individual is accurate and up-to-
14 date; and

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

18 (i) dispute the accuracy and complete-
19 ness of such personal data; and

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

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

1 vided in a manner that is appropriate and reason-
2 able based on the benefits and risks of harm to the
3 individual regarding the accuracy of the personal
4 data.

5 (3) EXCEPTIONS FOR PUBLICLY AVAILABLE IN-
6 FORMATION.—A covered entity shall not be required
7 to verify the accuracy of publicly available informa-
8 tion if the covered entity has reasonable procedures
9 to ensure that the publicly available information as-
10 sembled or maintained by the covered entity accu-
11 rately reflects the information available to the gen-
12 eral public.

13 (d) RIGHT TO ERASURE.—

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

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

1 account the amount of time that the entity requires
 2 to comply with the request considering the technical
 3 feasibility, cost, and burden to the entity of com-
 4 plying with the request.

5 (e) FREQUENCY AND COST TO EXERCISE RIGHTS.—

6 (1) IN GENERAL.—A covered entity—

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

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

17 (2) MANIFESTLY UNFOUNDED AND EXCESSIVE
 18 REQUESTS.—If an individual submits a manifestly
 19 unfounded or frivolous request to exercise a right
 20 under subsection (b), (c), or (d), or an excessive
 21 number of requests under such subsections, the cov-
 22 ered entity may—

23 (A) charge a reasonable fee, taking into ac-
 24 count the administrative costs of providing the

1 personal data, communication, or taking the ac-
2 tion requested by the individual; or

3 (B) refuse to act on the request.

4 (f) VERIFIED REQUEST.—

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

10 (2) VERIFICATION OF IDENTITY.—

11 (A) IN GENERAL.—A covered entity shall
12 make a reasonable effort to verify the identity
13 of any individual who submits a request to exer-
14 cise a right under this section.

15 (B) ADDITIONAL INFORMATION.—If a cov-
16 ered entity cannot verify the identity of the in-
17 dividual submitting a request under this sub-
18 section, the covered entity—

19 (i) may request that the individual
20 provide such additional information as is
21 necessary to confirm the identity of the in-
22 dividual; and

23 (ii) shall only process additional infor-
24 mation provided under clause (i) for the

1 purpose of verifying the identity of the in-
2 dividual.

3 (g) DECLINATION OF REQUESTS.—

4 (1) IN GENERAL.—A covered entity—

5 (A) shall decline to act on a request under
6 this section where, after undertaking a reason-
7 able effort, the entity cannot verify that the in-
8 dividual making the request is the individual
9 whose personal data is the subject of the re-
10 quest;

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

13 (i) require the covered entity or a
14 service provider of the covered entity to re-
15 tain any personal data collected for a sin-
16 gle, one-time transaction, if such personal
17 data is not processed for additional pur-
18 poses;

19 (ii) be impossible or demonstrably im-
20 practicable, or require any steps or meas-
21 ures to re-identify, or otherwise alter or
22 manipulate, information that is de-identi-
23 fied;

24 (iii) be contrary to the legitimate in-
25 terests of the covered entity or a service

1 provider of the covered entity, such as
2 completing a transaction, repairing func-
3 tionality or errors, or performing a con-
4 tract between the covered entity and the
5 individual;

6 (iv) impair the ability of the covered
7 entity or a service provider of the covered
8 entity to detect or respond to a security in-
9 cident, provide a secure environment, or
10 protect against malicious, deceptive, fraud-
11 ulent, or illegal activity;

12 (v) hinder compliance with a legal ob-
13 ligation or legally recognized privilege,
14 such as a requirement to retain certain in-
15 formation, or the establishment, exercise,
16 or defense of legal claims;

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

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

1 a reasonable individualized determination
 2 by the covered entity; and

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

6 (i) the covered entity requires the as-
 7 sistance of a service provider to fulfill the
 8 request; and

9 (ii) the service provider has informed
 10 the covered entity that the service provider
 11 is unable to assist the covered entity in ful-
 12 filling the request for a reason specified in
 13 section 8(c)(3)(A)(ii)(IV).

14 (2) NOTICE OF REASONS FOR DECLINATION.—

15 If the covered entity declines to act on a request
 16 pursuant to paragraph (1), the covered entity shall
 17 inform the individual who made the request of the
 18 reasons for such declination and any rights the indi-
 19 vidual may have to appeal the decision of the cov-
 20 ered entity.

21 (h) EXCEPTION FOR SMALL BUSINESSES.—The re-
 22 quirements under subsections (b) and (c) shall not apply
 23 to a covered entity that is a small business.

24 (i) GUIDANCE.—The Commission shall, after con-
 25 sulting with and soliciting comments from consumer data

1 industry representatives, issue guidance describing non-
 2 binding best practices for covered entities and service pro-
 3 viders of different business sizes and types to develop pri-
 4 vacy controls as described in this section.

5 **SEC. 6. SECURITY.**

6 (a) IN GENERAL.—Each covered entity and service
 7 provider shall develop, document, implement, and main-
 8 tain a comprehensive data security program that contains
 9 reasonable administrative, technical, and physical safe-
 10 guards designed to protect the security, confidentiality,
 11 and integrity of personal data from unauthorized access,
 12 use, destruction, acquisition, modification, or disclosure.

13 (b) CONSIDERATIONS OF SAFEGUARDS.—The safe-
 14 guards required under subsection (a) with respect to a cov-
 15 ered entity or service provider shall be appropriate to—

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

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

20 (3) the technical feasibility and cost of available
 21 tools, external audits or assessments, and other
 22 measures used by the covered entity or service pro-
 23 vider to improve security and reduce vulnerabilities;

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

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

6 (c) REQUIREMENTS FOR PROGRAM.—A comprehen-
7 sive data security program under this section shall be de-
8 signed to, at a minimum—

9 (1) designate an employee or employees to be
10 responsible for overseeing and maintaining its safe-
11 guards;

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

18 (A) employee training and management;

19 (B) information systems, including net-
20 work and software design, as well as informa-
21 tion processing, storage, transmission, and dis-
22 posal;

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

1 (D) whether the covered entity or service
2 provider has taken action to address and pre-
3 vent reasonably known and addressable security
4 vulnerabilities;

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

9 (4) maintain reasonable procedures to require
10 that third parties and service providers to whom per-
11 sonal data is transferred by the covered entity or
12 service provider involved maintain reasonable admin-
13 istrative, technical, and physical safeguards designed
14 to protect the security and confidentiality of per-
15 sonal data; and

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

21 **SEC. 7. ACCOUNTABILITY.**

22 (a) DEFINITION OF APPLICABLE ENTITY.—In this
23 section, the term “applicable entity” means a covered enti-
24 ty or service provider that, on an annual basis, conducts
25 collection and processing of—

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

3 (2) the sensitive personal data of more than
4 1,000,000 individuals.

5 (b) PRIVACY OFFICER.—

6 (1) DESIGNATION.—Each applicable entity
7 shall—

8 (A) designate an employee of the applica-
9 ble entity, or an individual who is a contractor
10 of the applicable entity, to be the privacy officer
11 responsible for overseeing its policies and prac-
12 tices relating to the collection and processing of
13 personal data; and

14 (B) ensure that the privacy officer is in-
15 volved in all issues relating to the privacy and
16 security of personal data.

17 (2) CONFLICTS OF INTEREST.—The privacy of-
18 ficer may perform other tasks and duties for the ap-
19 plicable entity, but only to the extent that the appli-
20 cable entity ensures that the performance of those
21 other tasks or duties does not present a conflict of
22 interest with respect to the duties and responsibil-
23 ities of the privacy officer role.

24 (3) RESPONSIBILITIES.—The privacy officer
25 shall—

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

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

6 (C) oversee—

7 (i) in the case of an applicable entity
 8 that is a covered entity, each privacy im-
 9 pact assessment carried out under sub-
 10 section (c); and

11 (ii) the comprehensive privacy pro-
 12 gram implemented under subsection (d);
 13 and

14 (D) act as a contact for the Commission,
 15 other Federal, State, and local authorities, and
 16 the applicable entity with respect to matters re-
 17 lating to the privacy and security of personal
 18 data.

19 (c) CONSIDERATION OF PRIVACY IMPLICATIONS OF
 20 MATERIAL CHANGES IN PROCESSING SENSITIVE PER-
 21 SONAL DATA.—

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

1 applicable entity shall, before beginning the new proc-
2 essing activity or making the material change, con-
3 sider the privacy implications, if any of the change.

4 (2) CONSIDERATIONS.—An applicable entity
5 that is a covered entity shall ensure, in considering
6 the privacy implications of a material change as re-
7 quired under paragraph (1), that the consideration
8 is reasonable and appropriate with respect to the
9 sensitive personal data that will be affected by the
10 new processing activity or the material change in
11 processing by considering—

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

14 (B) the potential for the new processing
15 activity or the material change to be a proxi-
16 mate cause of harm to individuals to whom the
17 sensitive personal data pertains.

18 (3) APPROVAL.—The privacy officer shall be re-
19 quired to approve the findings of a privacy impact
20 assessment carried out under paragraph (1) before
21 a applicable entity that is a covered entity may begin
22 the new processing activity or make the material
23 change that is the subject of the privacy impact as-
24 sessment.

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

8 (d) COMPREHENSIVE PRIVACY PROGRAM.—

9 (1) IN GENERAL.—Each applicable entity shall
 10 implement a comprehensive privacy program to safe-
 11 guard the privacy and security of personal data col-
 12 lected or processed by the applicable entity for the
 13 life cycle of development and operational practices of
 14 its products or services, including by—

15 (A) enhancing the privacy and security of
 16 personal data collected or processed by the ap-
 17 plicable entity through appropriate technical or
 18 operational safeguards, such as encryption, de-
 19 identification, and other privacy enhancing
 20 technologies;

21 (B) verifying that the applicable entity's
 22 practices relating to the collection and proc-
 23 essing of personal data are consistent with—

24 (i) the entity's policies and docu-
 25 mentation of such policies;

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

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

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

12 (i) in the case of an applicable entity
 13 that is a covered entity, each individual
 14 whose personal data is collected or proc-
 15 essed by the covered entity (excluding any
 16 personal data with respect to which the
 17 covered entity is a third party); and

18 (ii) in the case of an applicable entity
 19 that is a service provider, each covered en-
 20 tity to which the entity provides services.

21 (2) CONSIDERATIONS.—In implementing a com-
 22 prehensive privacy program under paragraph (1),
 23 each applicable entity shall—

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

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

(ii) the requirements under this Act;

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

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

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

SEC. 8. RULES RELATING TO SERVICE PROVIDERS.

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

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

(2) DUE DILIGENCE.—

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

4 (i) take reasonable steps to identify
5 whether the service provider has estab-
6 lished appropriate procedures and controls
7 for ensuring the privacy and security of
8 the personal data in a manner that com-
9 plies with the requirements of this Act, in-
10 cluding through reasonable representations
11 made to the covered entity by the service
12 provider in the contract governing the dis-
13 closure of personal data to the service pro-
14 vider; and

15 (ii) investigate any circumstances for
16 which a reasonable person would determine
17 that there is a high probability that the
18 service provider is not in compliance with
19 a requirement of this Act, and, if necessary
20 based on the findings of such investigation,
21 take reasonable steps to protect the pri-
22 vacy and security of any personal data dis-
23 closed by the covered entity to the service
24 provider that is at risk as a result of the

1 service provider's noncompliance with a re-
 2 quirement of this Act.

3 (B) CONSIDERATIONS.—In determining
 4 whether a covered entity has acted reasonably
 5 in complying with clause (i) or (ii) of subpara-
 6 graph (A), the Commission shall take into ac-
 7 count—

8 (i) the size, complexity, and resources
 9 of the covered entity and whether the cov-
 10 ered entity is a small business; and

11 (ii) the risk of harm reasonably ex-
 12 pected to occur as a result of the covered
 13 entity disclosing personal data to a service
 14 provider without complying with such
 15 clause.

16 (b) CONTRACTUAL REQUIREMENTS.—

17 (1) IN GENERAL.—A contract between a cov-
 18 ered entity and a service provider governing the dis-
 19 closure of personal data by the covered entity to the
 20 service provider shall—

21 (A) require the service provider to only col-
 22 lect or process the personal data as directed by
 23 the covered entity;

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

1 data by the service provider, including instruc-
2 tions, policies, and practices, as applicable, with
3 which the service provider is required to com-
4 ply; and

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

10 (2) LIMITATION.—No contract governing the
11 disclosure of personal data by a covered entity to a
12 service provider shall relieve a covered entity or serv-
13 ice provider of any requirement or obligation with
14 respect to such personal data that is imposed on the
15 covered entity or service provider, as applicable, by
16 this Act.

17 (c) SERVICE PROVIDER OBLIGATIONS.—

18 (1) NOTICE OF PROCESSING OF PERSONAL
19 DATA TO COMPLY WITH LEGAL REQUIREMENT.—In
20 the event that a service provider is required to proc-
21 ess personal data in order to comply with a legal re-
22 quirement, including a subpoena, summons, or other
23 properly executed compulsory process, the service
24 provider shall inform the covered entity from which
25 it received the personal data involved of such legal

1 requirement before such processing, unless the serv-
2 ice provider is otherwise prohibited by law from pro-
3 viding such notification.

4 (2) NOTICE OF CHANGE TO POLICIES OR PRAC-
5 TICES.—If a service provider amends its policies or
6 practices relating to personal data in a manner that
7 is relevant to compliance with any provision of this
8 Act, the service provider shall provide reasonable no-
9 tice in advance of such change to any covered entity
10 on whose behalf the service provider collects or proc-
11 esses personal data.

12 (3) RESPONSIBILITIES.—

13 (A) INDIVIDUAL CONTROL REQUESTS.—A
14 service provider that collects or processes per-
15 sonal data on behalf of a covered entity shall,
16 to the extent possible, either—

17 (i) provide the covered entity with ap-
18 propriate technical and organizational
19 measures to enable the covered entity to
20 comply with requests to exercise rights de-
21 scribed in section 5 with respect to any
22 such personal data that is held by, and
23 reasonably accessible to, the service pro-
24 vider; or

1 (ii) respond to any request made by
2 the covered entity for assistance in com-
3 plying with a request to exercise such a
4 right with respect to such personal data
5 that the covered entity has verified as de-
6 scribed in section 5(f) and has determined
7 must be complied with under this Act by,
8 as appropriate—

9 (I) in the case of a request de-
10 scribed in subsection (b) of section 5,
11 providing the covered entity with ac-
12 cess to any relevant personal data
13 held by, and reasonably available to,
14 the service provider;

15 (II) in the case of a request de-
16 scribed in subsection (c) of such sec-
17 tion, by correcting any relevant per-
18 sonal data held by, and reasonably ac-
19 cessible to, the service provider, and
20 providing the covered entity with no-
21 tice of such correction;

22 (III) in the case of a request de-
23 scribed in subsection (d) of such sec-
24 tion, by deleting, de-identifying, or re-
25 turning to the covered entity any rel-

1 evant personal data held by, and rea-
 2 sonably accessible to, the service pro-
 3 vider, and providing the covered entity
 4 with notice of such action; or

5 (IV) informing the covered entity
 6 that—

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

10 (bb) the service provider
 11 cannot reasonably access any
 12 personal data related to the re-
 13 quest; or

14 (cc) complying with the re-
 15 quest would be inconsistent with
 16 a legal requirement to which the
 17 service provider is subject.

18 (B) DELETION OF DATA UPON COMPLE-
 19 TION OF SERVICE.—Except as otherwise re-
 20 quired by law, as soon as practicable after the
 21 completion of the service or function for which
 22 a service provider collected or processed per-
 23 sonal data on behalf of a covered entity, the
 24 service provider shall delete, de-identify, or re-

1 turn to the covered entity all such personal
2 data.

3 (C) ASSURANCE OF COMPLIANCE.—

4 (i) IN GENERAL.—Subject to clause
5 (ii), a service provider shall make available
6 to a covered entity on whose behalf the
7 service provider collects or processes per-
8 sonal data information necessary to dem-
9 onstrate the service provider's compliance
10 with subparagraph (A).

11 (ii) WRITTEN REPRESENTATION OF
12 COMPLIANCE.—If the information de-
13 scribed in clause (i) is not technically avail-
14 able to a service provider, the service pro-
15 vider may comply with clause (i) by pro-
16 viding the covered entity with a written
17 representation stating that the service pro-
18 vider is in compliance with subparagraph
19 (A).

20 (4) SUBCONTRACTOR REQUIREMENTS.—A serv-
21 ice provider that is collecting or processing personal
22 data on behalf of a covered entity shall not employ
23 a subcontractor to carry out or assist in such collec-
24 tion or processing unless—

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

4 (B) the subcontractor is subject (pursuant
 5 to an agreement between the service provider
 6 and the subcontractor) to the same require-
 7 ments and obligations as the service provider
 8 with respect to the collection and processing of
 9 the personal data.

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

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

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

20 **SEC. 9. ENFORCEMENT.**

21 (a) ENFORCEMENT BY THE COMMISSION.—

22 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
 23 TICES.—A violation of this Act or a regulation pro-
 24 mulgated under this Act shall be treated as an un-
 25 fair or deceptive act or practice in violation of a rule

1 promulgated under section 18(a)(1)(B) of the Fed-
2 eral Trade Commission Act (15 U.S.C.
3 57a(a)(1)(B)).

4 (2) POWERS OF THE COMMISSION.—

5 (A) IN GENERAL.—Except as provided in
6 subparagraph (C), the Commission shall enforce
7 this Act and any regulation promulgated under
8 this Act in the same manner, by the same
9 means, and with the same jurisdiction, powers,
10 and duties as though all applicable terms and
11 provisions of the Federal Trade Commission
12 Act (15 U.S.C. 41 et seq.) were incorporated
13 into and made a part of this Act.

14 (B) PRIVILEGES AND IMMUNITIES.—Any
15 covered entity or service provider who violates
16 this Act or a regulation promulgated under this
17 Act shall be subject to the penalties and enti-
18 tled to the privileges and immunities provided
19 in the Federal Trade Commission Act (15
20 U.S.C. 41 et seq.).

21 (C) COMMON CARRIERS AND NONPROFIT
22 ORGANIZATIONS.—Notwithstanding section 4,
23 5(a)(2), or 6 of the Federal Trade Commission
24 Act (15 U.S.C. 44, 45(a)(2), 46) or any juris-
25 dictional limitation of the Commission, the

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

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

(3) CIVIL PENALTIES.—

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

(B) AMOUNT.—

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

1 penalty described in subparagraph (A)
2 shall be the number of individuals affected
3 by a violation described in that subpara-
4 graph multiplied by an amount not to ex-
5 ceed \$42,530.

6 (ii) CONSIDERATIONS.—In deter-
7 mining the amount of a civil penalty to
8 seek under subparagraph (A) for a viola-
9 tion described in that subparagraph, the
10 Commission shall consider, with respect to
11 the covered entity or service provider that
12 committed the violation—

13 (I) the degree of harm associated
14 with the privacy and security of per-
15 sonal data of individuals created by
16 the violation;

17 (II) the intent of the covered en-
18 tity or service provider in committing
19 the violation;

20 (III) the size, complexity, and re-
21 sources of the covered entity or serv-
22 ice provider, including if it is a small
23 business;

1 (IV) reasonable expectations re-
 2 lating to privacy and security of per-
 3 sonal data of individuals;

4 (V) the degree to which the cov-
 5 ered entity or service provider put in
 6 place appropriate controls or complied
 7 with the requirements of section 7, if
 8 applicable;

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

12 (VII) what, if any, efforts the
 13 covered entity or service provider has
 14 taken to mitigate any risk to the pri-
 15 vacy and security of personal data of
 16 individuals created by the processing.

17 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-
 18 ERAL.—

19 (1) CIVIL ACTION.—In any case in which an at-
 20 torney general of a State has reason to believe that
 21 an interest of the residents of that State has been
 22 or is threatened or adversely affected by the engage-
 23 ment of any covered entity or service provider in a
 24 practice that violates this Act or a regulation pro-
 25 mulgated under this Act, the attorney general of the

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

4 (A) enjoin that practice;

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

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

10 (2) RIGHTS OF THE COMMISSION.—

11 (A) NOTICE TO COMMISSION.—

12 (i) IN GENERAL.—Except as provided
 13 in clause (iii), the attorney general of a
 14 State shall notify the Commission in writ-
 15 ing that the attorney general intends to
 16 bring a civil action under paragraph (1)
 17 not later than 10 days before initiating the
 18 civil action.

19 (ii) CONTENTS.—The notification re-
 20 quired by clause (i) with respect to a civil
 21 action shall include a copy of the complaint
 22 to be filed to initiate the civil action.

23 (iii) EXCEPTION.—If it is not feasible
 24 for the attorney general of a State to pro-
 25 vide the notification required by clause (i)

1 before initiating a civil action under para-
2 graph (1), the attorney general shall notify
3 the Commission immediately upon insti-
4 tuting the civil action.

5 (B) INTERVENTION BY THE COMMIS-
6 SION.—The Commission may—

- 7 (i) intervene in any civil action
8 brought by the attorney general of a State
9 under paragraph (1); and
10 (ii) upon intervening under clause
11 (i)—

12 (I) be heard on all matters aris-
13 ing in the civil action; and

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

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

18 (A) IN GENERAL.—Subject to subpara-
19 graph (B), if a civil action under paragraph (1)
20 is pending in a district court of the United
21 States and one or more civil actions are com-
22 menced pursuant to paragraph (1) in a dif-
23 ferent district court of the United States that
24 involve one or more common questions of fact,
25 all such civil actions shall be transferred for the

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

4 (B) EXCEPTION.—A civil action shall not
5 be transferred pursuant to subparagraph (A) if
6 pretrial proceedings in such civil action have
7 concluded before the subsequent action is com-
8 menced pursuant to paragraph (1).

9 (c) LIMITATION ON STATE ACTION WHILE FEDERAL
10 ACTION IS PENDING.—If the Commission institutes an
11 action under subsection (a) with respect to a violation of
12 this Act or a regulation promulgated under this Act, a
13 State may not, during the pendency of that action, insti-
14 tute an action under subsection (b) 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 (d) NO PRIVATE RIGHT OF ACTION.—There shall be
20 no private right of action under this Act and nothing in
21 this Act may be construed to provide a basis for a private
22 right of action.

23 **SEC. 10. RELATION TO OTHER LAWS.**

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

1 of Congress to promote consistency in consumer expecta-
2 tions, competitive parity, and innovation through the es-
3 tablishment of a uniform Federal privacy framework that
4 preempts, and occupies the field with respect to, the au-
5 thority of any State or political subdivision of a State over
6 the conduct or activities of covered entities covered by this
7 Act (or under a law enumerated in subsection (c)) relating
8 to the privacy or security of personal data, including con-
9 sumer controls relating to personal data such as rights
10 to access, correction, and deletion.

11 (b) EXPRESS PREEMPTION OF STATE LAW.—

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

18 (2) PRESERVATION OF STATE AND LOCAL
19 LAWS.—The provisions of this Act shall not be con-
20 strued to preempt or supersede the applicability of
21 any of the following laws of a State or political sub-
22 division of a State to the extent that such law is not
23 inconsistent with this Act:

24 (A) Laws that address notification require-
25 ments in the event of a data breach.

1 (B) Rules of criminal or civil procedure.

2 (C) Laws that relate to the general stand-
3 ards of fraud or public safety.

4 (D) Laws that address the privacy of any
5 group of students (as defined in section 444(a)
6 of the General Education Provisions Act (20
7 U.S.C. 1232g(a)) (commonly referred to as the
8 “Family Educational Rights and Privacy Act of
9 1974”)).

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

14 (F) Laws that address protected health in-
15 formation held by covered entities and business
16 associates (as such terms are defined for pur-
17 poses of regulations promulgated under section
18 264(c) of the Health Insurance Portability and
19 Accountability Act of 1996 (42 U.S.C. 1320d–
20 2 note)).

21 (G) Laws governing employment and em-
22 ployment-related data including data collected
23 or used by an employer pursuant to an em-
24 ployer-employee relationship.

1 (H) Laws protecting the right of individ-
2 uals to be free of discrimination based on race,
3 sex, national origin, or other suspect classifica-
4 tion identified under State law.

5 (c) RELATION TO OTHER FEDERAL LAWS.—

6 (1) IN GENERAL.—Except as otherwise pro-
7 vided in paragraphs (2) and (4), this Act shall su-
8 persede any other Federal statute or regulation re-
9 lating to the privacy or security of personal data.

10 (2) SAVINGS PROVISION.—This Act shall not be
11 construed to modify, limit, or supersede the oper-
12 ation of any of the following laws:

13 (A) The Children’s Online Privacy Protec-
14 tion Act (15 U.S.C. 6501 et seq.).

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

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

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

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

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

1 (G) The Health Information Technology
2 for Economic and Clinical Health Act (42
3 U.S.C. 17931 et seq.).

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

8 (I) The Electronic Communications Pri-
9 vacy Act (18 U.S.C. 2510 et seq.).

10 (J) The Driver’s Privacy Protection Act of
11 1994 (18 U.S.C. 2721 et seq.).

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

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

21 (4) NONAPPLICATION OF FCC LAWS AND REGU-
22 LATIONS TO COVERED ENTITIES.—Notwithstanding
23 any other provision of law, neither any provision of
24 the Communications Act of 1934 (47 U.S.C. 151 et
25 seq.) and all Acts amendatory thereof and supple-

1 mentary thereto nor any regulation promulgated by
2 the Federal Communications Commission under
3 such Acts shall apply to any covered entity with re-
4 spect to the collection, use, processing, transferring,
5 or security of personal data, except to the extent
6 that such provision or regulation pertains solely to
7 “911” lines or any other emergency line of a hos-
8 pital, medical provider or service office, health care
9 facility, poison control center, fire protection agency,
10 or law enforcement agency.

11 **SEC. 11. COMMISSION RESOURCES.**

12 (a) APPOINTMENT OF ATTORNEYS, TECHNOLOGISTS,
13 AND SUPPORT PERSONNEL.—Notwithstanding any other
14 provision of law, the Chair of the Commission shall ap-
15 point no fewer than 440 additional individuals to serve as
16 personnel to enforce this Act and other laws relating to
17 privacy and data security that the Commission is author-
18 ized to enforce.

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

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

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

3 (A) that are not available to the Commis-
4 sion; and

5 (B) that the Commission requires to effec-
6 tively carry out this Act.

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

10 **SEC. 12. GUIDANCE AND REPORTING.**

11 (a) INTERNATIONAL COORDINATION AND COOPERA-
12 TION.—

13 (1) IN GENERAL.—If necessary, the Commis-
14 sion shall coordinate any enforcement action by the
15 Commission under this Act with any relevant data
16 protection authority established by a foreign country
17 or any similar office of a foreign country in a man-
18 ner consistent with subsections (j) and (k) of section
19 6 of the Federal Trade Commission Act (15 U.S.C.
20 46).

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

1 (A) identify laws of foreign countries or re-
2 gions that relate to the processing of personal
3 data for commercial purposes;

4 (B) engage with relevant officials of for-
5 eign countries or regions that have implemented
6 laws described in subparagraph (A) in order to
7 identify requirements under those laws that
8 could disrupt cross-border transfers of personal
9 data;

10 (C) develop mechanisms and recommenda-
11 tions to prevent disruptions described in sub-
12 paragraph (B); and

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

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

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

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

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

5 (4) enforcement actions by the Commission and
6 State attorneys general for violations of the provi-
7 sions of this Act and regulations promulgated under
8 this Act;

9 (5) priorities of the Commission in enforcing
10 the provisions of this Act and regulations promul-
11 gated under this Act; and

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

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

22 (1) identify any inconsistency between the re-
23 quirements under this Act and the requirements
24 under any law related to the privacy and security of
25 personal data;

1 (2) review the impact of the provisions of this
2 Act on small businesses and provide recommenda-
3 tions, if necessary, to improve compliance and en-
4 forcement;

5 (3) provide recommendations on amending Fed-
6 eral data privacy and security laws in light of chang-
7 ing technological and economic trends; and

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

11 **SEC. 13. SEVERABILITY.**

12 If any provision of this Act or the application of such
13 provision to any person or circumstance is held to be un-
14 constitutional, the remainder of this Act, and the applica-
15 tion of the provision to any other person or circumstance,
16 shall not be affected.

17 **SEC. 14. EFFECTIVE DATE.**

18 This Act shall take effect on the date that is 1 year
19 after the date of enactment of this Act, except that section
20 10 shall take effect upon the date of enactment of this
21 Act.

