

AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 8152
OFFERED BY M. _____

Strike all after the enacting clause and insert the following:

1 SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the
“American Data Privacy and Protection Act”.

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

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.

TITLE I—DUTY OF LOYALTY

Sec. 101. Data minimization.
 Sec. 102. Loyalty duties.
 Sec. 103. Privacy by design.
 Sec. 104. Loyalty to individuals with respect to pricing.

TITLE II—CONSUMER DATA RIGHTS

- Sec. 201. Consumer awareness.
- Sec. 202. Transparency.
- Sec. 203. Individual data ownership and control.
- Sec. 204. Right to consent and object.
- Sec. 205. Data protections for children and minors.
- Sec. 206. Third-party collecting entities.
- Sec. 207. Civil rights and algorithms.
- Sec. 208. Data security and protection of covered data.
- Sec. 209. Small business protections.
- Sec. 210. Unified opt-out mechanisms.

TITLE III—CORPORATE ACCOUNTABILITY

Sec. 301. Executive responsibility.

Sec. 302. Technical compliance programs.

Sec. 303. Commission approved compliance guidelines.

Sec. 304. Digital content forgeries.

TITLE IV—ENFORCEMENT, APPLICABILITY, AND MISCELLANEOUS

Sec. 401. Enforcement by the Federal Trade Commission.

Sec. 402. Enforcement by States.

Sec. 403. Enforcement by persons.

Sec. 404. Relationship to Federal and State laws.

Sec. 405. Severability.

Sec. 406. COPPA.

Sec. 407. Authorization of appropriations.

Sec. 408. Effective date.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) **AFFIRMATIVE EXPRESS CONSENT.**—

4 (A) **IN GENERAL.**—The term “affirmative
5 express consent” means an affirmative act by
6 an individual that clearly communicates the in-
7 dividual’s freely given, specific, and unambig-
8 uous authorization for an act or practice after
9 having been informed, in response to a specific
10 request from a covered entity that meets the re-
11 quirements of subparagraph (B).

12 (B) **REQUEST REQUIREMENTS.**—The re-
13 quirements of this subparagraph with respect to
14 a request from a covered entity to an individual
15 are the following:

16 (i) The request is provided to the indi-
17 vidual in a clear and conspicuous stand-
18 alone disclosure made through the primary
19 medium used to offer the covered entity’s
20 product or service, or only if the product
21 or service is not offered in a medium that

1 permits the making of the request under
2 this paragraph, another medium regularly
3 used in conjunction with the covered enti-
4 ty's product or service.

5 (ii) The request includes a description
6 of the processing purpose for which the in-
7 dividual's consent is sought and—

8 (I) clearly states the specific cat-
9 egories of covered data that the cov-
10 ered entity shall collect, process, and
11 transfer necessary to effectuate the
12 processing purpose; and

13 (II) includes a prominent heading
14 and is written in easy-to-understand
15 language that would enable a reason-
16 able individual to identify and under-
17 stand the processing purpose for
18 which consent is sought and the cov-
19 ered data to be collected, processed, or
20 transferred by the covered entity for
21 such processing purpose.

22 (iii) The request clearly explains the
23 individual's applicable rights related to
24 consent.

1 (iv) The request is made in a manner
2 reasonably accessible to and usable by indi-
3 viduals with disabilities.

4 (v) The request is made available to
5 the individual in each covered language in
6 which the covered entity provides a product
7 or service for which authorization is
8 sought.

9 (vi) The option to refuse consent shall
10 be at least as prominent as the option to
11 accept, and the option to refuse consent
12 shall take the same number of steps or
13 fewer as the option to accept.

14 (vii) Processing or transferring any
15 covered data collected pursuant to affirma-
16 tive express consent for a different proc-
17 essing purpose than that for which affirm-
18 ative express consent was obtained shall
19 require affirmative express consent for the
20 subsequent processing purpose.

21 (C) EXPRESS CONSENT REQUIRED.—A
22 covered entity may not infer that an individual
23 has provided affirmative express consent to an
24 act or practice from the inaction of the indi-
25 vidual or the individual's continued use of a

1 service or product provided by the covered enti-
2 ty.

3 (D) PRETEXTUAL CONSENT PROHIB-
4 ITED.—A covered entity may not obtain or at-
5 tempt to obtain the affirmative express consent
6 of an individual through—

7 (i) the use of any false, fictitious,
8 fraudulent, or materially misleading state-
9 ment or representation; or

10 (ii) the design, modification, or ma-
11 nipulation of any user interface with the
12 purpose or substantial effect of obscuring,
13 subverting, or impairing a reasonable indi-
14 vidual’s autonomy, decision making, or
15 choice to provide such consent or any cov-
16 ered data.

17 (2) AUTHENTICATION.—The term “authentica-
18 tion” means the process of verifying an individual or
19 entity for security purposes.

20 (3) BIOMETRIC INFORMATION.—

21 (A) IN GENERAL.—The term “biometric
22 information” means any covered data generated
23 from the technological processing of an individ-
24 ual’s unique biological, physical, or physiological

1 characteristics that is linked or reasonably
2 linkable to an individual, including—

- 3 (i) fingerprints;
4 (ii) voice prints;
5 (iii) iris or retina scans;
6 (iv) facial or hand mapping, geometry,
7 or templates; or
8 (v) gait or personally identifying phys-
9 ical movements.

10 (B) EXCLUSION.—The term “biometric in-
11 formation” does not include—

- 12 (i) a digital or physical photograph;
13 (ii) an audio or video recording; or
14 (iii) data generated from a digital or
15 physical photograph, or an audio or video
16 recording, that cannot be used to identify
17 an individual.

18 (4) COLLECT; COLLECTION.—The terms “col-
19 lect” and “collection” mean buying, renting, gath-
20 ering, obtaining, receiving, accessing, or otherwise
21 acquiring covered data by any means.

22 (5) COMMISSION.—The term “Commission”
23 means the Federal Trade Commission.

24 (6) CONTROL.—The term “control” means,
25 with respect to an entity—

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

4 (B) control over the election of a majority
5 of the directors of the entity (or of individuals
6 exercising similar functions); or

7 (C) the power to exercise a controlling in-
8 fluence over the management of the entity.

9 (7) COVERED ALGORITHM.—The term “covered
10 algorithm” means a computational process that uses
11 machine learning, natural language processing, arti-
12 ficial intelligence techniques, or other computational
13 processing techniques of similar or greater com-
14 plexity and that makes a decision or facilitates
15 human decision-making with respect to covered data,
16 including to determine the provision of products or
17 services or to rank, order, promote, recommend, am-
18 plify, or similarly determine the delivery or display
19 of information to an individual.

20 (8) COVERED DATA.—

21 (A) IN GENERAL.—The term “covered
22 data” means information that identifies or is
23 linked or reasonably linkable, alone or in com-
24 bination with other information, to an indi-
25 vidual or a device that identifies or is linked or

1 reasonably linkable to an individual, and may
2 include derived data and unique persistent identifiers.
3

4 (B) EXCLUSIONS.—The term “covered
5 data” does not include—

6 (i) de-identified data;

7 (ii) employee data;

8 (iii) publicly available information; or

9 (iv) inferences made exclusively from
10 multiple independent sources of publicly
11 available information that do not reveal
12 sensitive covered data with respect to an
13 individual.

14 (C) EMPLOYEE DATA DEFINED.—For purposes of subparagraph (B), the term “employee
15 data” means—
16

17 (i) information relating to a job applicant collected by a covered entity acting as
18 a prospective employer of such job applicant in the course of the application, or
19 hiring process, if such information is collected, processed, or transferred by the
20 prospective employer solely for purposes
21 related to the employee’s status as a cur-
22
23
24

1 rent or former job applicant of such em-
2 ployer;

3 (ii) information processed by an em-
4 ployer relating to an employee who is act-
5 ing in a professional capacity for the em-
6 ployer, provided that such information is
7 collected, processed, or transferred solely
8 for purposes related to such employee's
9 professional activities on behalf of the em-
10 ployer;

11 (iii) the business contact information
12 of an employee, including the employee's
13 name, position or title, business telephone
14 number, business address, or business
15 email address that is provided to an em-
16 ployer by an employee who is acting in a
17 professional capacity, if such information
18 is collected, processed, or transferred solely
19 for purposes related to such employee's
20 professional activities on behalf of the em-
21 ployer;

22 (iv) emergency contact information
23 collected by an employer that relates to an
24 employee of that employer, if such infor-
25 mation is collected, processed, or trans-

ferred solely for the purpose of having an emergency contact on file for the employee and for processing or transferring such information in case of an emergency; or

(v) information relating to an employee (or a spouse, dependent, other covered family member, or beneficiary of such employee) that is necessary for the employer to collect, process, or transfer solely for the purpose of administering benefits to which such employee (or spouse, dependent, other covered family member, or beneficiary of such employee) is entitled on the basis of the employee's position with that employer.

(9) COVERED ENTITY.—

(A) IN GENERAL.—The term “covered entity”—

(i) means any entity or any person, other than an individual acting in a non-commercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data and—

1 (I) is subject to the Federal
2 Trade Commission Act (15 U.S.C. 41
3 et seq.);

4 (II) is a common carrier subject
5 to the Communications Act of 1934
6 (47 U.S.C. 151 et seq.) and all Acts
7 amendatory thereof and supple-
8 mentary thereto; or

9 (III) is an organization not orga-
10 nized to carry on business for its own
11 profit or that of its members; and

12 (ii) includes any entity or person that
13 controls, is controlled by, or is under com-
14 mon control with the covered entity.

15 (B) EXCLUSIONS.—The term “covered en-
16 tity” does not include—

17 (i) a Federal, State, Tribal, territorial,
18 or local government entity such as a body,
19 authority, board, bureau, commission, dis-
20 trict, agency, or political subdivision of the
21 Federal Government or a State, Tribal,
22 territorial, or local government; or

23 (ii) a person or an entity that is col-
24 lecting, processing, or transferring covered
25 data on behalf of a Federal, State, Tribal,

1 territorial, or local government entity, in so
2 far as such person or entity is acting as a
3 service provider to the government entity.

4 (C) NON-APPLICATION TO SERVICE PRO-
5 VIDERS.—An entity shall not be considered to
6 be a covered entity for purposes of this Act in
7 so far as the entity is acting as a service pro-
8 vider (as defined in paragraph (29)).

9 (10) COVERED LANGUAGE.—The term “covered
10 language” means the ten languages with the most
11 users in the United States, according to the most re-
12 cent United States Census.

13 (11) COVERED MINOR.—The term “covered
14 minor” means an individual under the age of 17.

15 (12) DE-IDENTIFIED DATA.—The term “de-
16 identified data” means information that does not
17 identify and is not linked or reasonably linkable to
18 a distinct individual or a device, regardless of wheth-
19 er the information is aggregated, and if the covered
20 entity or service provider—

21 (A) takes reasonable technical measures to
22 ensure that the information cannot, at any
23 point, be used to re-identify any individual or
24 device that identifies or is linked or reasonably
25 linkable to an individual;

1 (B) publicly commits in a clear and con-
2 spicuous manner—

3 (i) to process and transfer the infor-
4 mation solely in a de-identified form with-
5 out any reasonable means for re-identifica-
6 tion; and

7 (ii) to not attempt to re-identify the
8 information with any individual or device
9 that identifies or is linked or reasonably
10 linkable to an individual; and

11 (C) contractually obligates any person or
12 entity that receives the information from the
13 covered entity or service provider—

14 (i) to comply with all of the provisions
15 of this paragraph with respect to the infor-
16 mation; and

17 (ii) to require that such contractual
18 obligations be included contractually in all
19 subsequent instances for which the data
20 may be received.

21 (13) DERIVED DATA.—The term “derived data”
22 means covered data that is created by the derivation
23 of information, data, assumptions, correlations, in-
24 ferences, predictions, or conclusions from facts, evi-

1 dence, or another source of information or data
2 about an individual or an individual’s device.

3 (14) DEVICE.—The term “device” means any
4 electronic equipment capable of collecting, proc-
5 essing, or transferring covered data that is used by
6 one or more individuals.

7 (15) EMPLOYEE.—The term “employee” means
8 an individual who is an employee, director, officer,
9 staff member individual working as an independent
10 contractor that is not a service provider, trainee, vol-
11 unteer, or intern of an employer, regardless of
12 whether such individual is paid, unpaid, or employed
13 on a temporary basis.

14 (16) EXECUTIVE AGENCY.—The “Executive
15 agency” has the meaning given such term in section
16 105 of title 5, United States Code.

17 (17) FIRST PARTY ADVERTISING OR MAR-
18 KETING.—The term “first party advertising or mar-
19 keting” means advertising or marketing conducted
20 by a first party either through direct communica-
21 tions with a user such as direct mail, email, or text
22 message communications, or advertising or mar-
23 keting conducted entirely within the first-party con-
24 text, such as in a physical location operated by the

1 first party, or on a web site or app operated by the
2 first party.

3 (18) GENETIC INFORMATION.—The term “ge-
4 netic information” means any covered data, regard-
5 less of its format, that concerns an individual’s ge-
6 netic characteristics, including—

7 (A) raw sequence data that results from
8 the sequencing of the complete, or a portion of
9 the, extracted deoxyribonucleic acid (DNA) of
10 an individual; or

11 (B) genotypic and phenotypic information
12 that results from analyzing raw sequence data
13 described in subparagraph (A).

14 (19) INDIVIDUAL.—The term “individual”
15 means a natural person residing in the United
16 States.

17 (20) KNOWLEDGE.—

18 (A) IN GENERAL.—The term “knowledge”
19 means—

20 (i) with respect to a covered entity
21 that is a covered high-impact social media
22 company, the entity knew or should have
23 known the individual was a covered minor;

24 (ii) with respect to a covered entity or
25 service provider that is a large data holder,

1 and otherwise is not a covered high-impact
2 social media company, that the covered en-
3 tity knew or acted in willful disregard of
4 the fact that the individual was a covered
5 minor; and

6 (iii) with respect to a covered entity or
7 service provider that does not meet the re-
8 quirements of clause (i) or (ii), actual
9 knowledge.

10 (B) COVERED HIGH-IMPACT SOCIAL MEDIA
11 COMPANY.—For purposes of this paragraph, the
12 term “covered high-impact social media com-
13 pany” means a covered entity that provides any
14 internet-accessible platform where—

15 (i) such covered entity generates
16 \$3,000,000,000 or more in annual revenue;

17 (ii) such platform has 300,000,000 or
18 more monthly active users for not fewer
19 than 3 of the preceding 12 months on the
20 online product or service of such covered
21 entity; and

22 (iii) such platform constitutes an on-
23 line product or service that is primarily
24 used by users to access or share, user-gen-
25 erated content.

1 (21) LARGE DATA HOLDER.—

2 (A) IN GENERAL.—The term “large data
3 holder” means a covered entity or service pro-
4 vider that, in the most recent calendar year—

5 (i) had annual gross revenues of
6 \$250,000,000 or more; and

7 (ii) collected, processed, or trans-
8 ferred—

9 (I) the covered data of more than
10 5,000,000 individuals or devices that
11 identify or are linked or reasonably
12 linkable to 1 or more individuals, ex-
13 cluding covered data collected and
14 processed solely for the purpose of ini-
15 tiating, rendering, billing for, final-
16 izing, completing, or otherwise col-
17 lecting payment for a requested prod-
18 uct or service; and

19 (II) the sensitive covered data of
20 more than 200,000 individuals or de-
21 vices that identify or are linked or
22 reasonably linkable to 1 or more indi-
23 viduals.

24 (B) EXCLUSIONS.—The term “large data
25 holder” does not include any instance in which

1 the covered entity or service provider would
2 qualify as a large data holder solely on the
3 basis of collecting or processing—

- 4 (i) personal email addresses;
- 5 (ii) personal telephone numbers; or
- 6 (iii) log-in information of an indi-
7 vidual or device to allow the individual or
8 device to log in to an account administered
9 by the covered entity or service provider.

10 (C) REVENUE.—For purposes of deter-
11 mining whether any covered entity or service
12 provider is a large data holder, the term “rev-
13 enue”, with respect to any covered entity or
14 service provider that is not organized to carry
15 on business for its own profit or that of its
16 members—

- 17 (i) means the gross receipts the cov-
18 ered entity or service provider received, in
19 whatever form, from all sources, without
20 subtracting any costs or expenses; and
- 21 (ii) includes contributions, gifts,
22 grants, dues or other assessments, income
23 from investments, and proceeds from the
24 sale of real or personal property.

1 (22) MARKET RESEARCH.—The term “market
2 research” means the collection, processing, or trans-
3 fer of covered data as reasonably necessary and pro-
4 portionate to investigate the market for or mar-
5 keting of products, services, or ideas, where the cov-
6 ered data is not—

7 (A) integrated into any product or service;

8 (B) otherwise used to contact any indi-
9 vidual or individual’s device; or

10 (C) used to advertise or market to any in-
11 dividual or individual’s device.

12 (23) MATERIAL.—The term “material” means,
13 with respect to an act, practice, or representation of
14 a covered entity (including a representation made by
15 the covered entity in a privacy policy or similar dis-
16 closure to individuals) involving the collection, proc-
17 essing, or transfer of covered data, that such act,
18 practice, or representation is likely to affect a rea-
19 sonable individual’s decision or conduct regarding a
20 product or service.

21 (24) PRECISE GEOLOCATION INFORMATION.—

22 (A) IN GENERAL.—The term “precise
23 geolocation information” means information
24 that is derived from a device or technology that
25 reveals the past or present physical location of

1 an individual or device that identifies or is
2 linked or reasonably linkable to 1 or more indi-
3 viduals, with sufficient precision to identify
4 street level location information of an individual
5 or device or the location of an individual or de-
6 vice within a range of 1,850 feet or less.

7 (B) EXCLUSION.—The term “precise
8 geolocation information” does not include
9 geolocation information identifiable or derived
10 solely from the visual content of a legally ob-
11 tained image, including the location of the de-
12 vice that captured such image.

13 (25) PROCESS.—The term “process” means to
14 conduct or direct any operation or set of operations
15 performed on covered data, including analyzing, or-
16 ganizing, structuring, retaining, storing, using, or
17 otherwise handling covered data.

18 (26) PROCESSING PURPOSE.—The term “proc-
19 essing purpose” means a reason for which a covered
20 entity or service provider collects, processes, or
21 transfers covered data that is specific and granular
22 enough for a reasonable individual to understand the
23 material facts of how and why the covered entity or
24 service provider collects, processes, or transfers the
25 covered data.

1 (27) PUBLICLY AVAILABLE INFORMATION.—

2 (A) IN GENERAL.—The term “publicly
3 available information” means any information
4 that a covered entity or service provider has a
5 reasonable basis to believe has been lawfully
6 made available to the general public from—

7 (i) Federal, State, or local government
8 records, if the covered entity collects, proc-
9 esses, and transfers such information in
10 accordance with any restrictions or terms
11 of use placed on the information by the rel-
12 evant government entity;

13 (ii) widely distributed media;

14 (iii) a website or online service made
15 available to all members of the public, for
16 free or for a fee, including where all mem-
17 bers of the public, for free or for a fee, can
18 log in to the website or online service;

19 (iv) a disclosure that has been made
20 to the general public as required by Fed-
21 eral, State, or local law; or

22 (v) the visual observation of the phys-
23 ical presence of an individual or a device in
24 a public place, not including data collected
25 by a device in the individual’s possession.

1 (B) CLARIFICATIONS; LIMITATIONS.—

2 (i) AVAILABLE TO ALL MEMBERS OF
3 THE PUBLIC.—For purposes of this para-
4 graph, information from a website or on-
5 line service is not available to all members
6 of the public if the individual who made
7 the information available via the website or
8 online service has restricted the informa-
9 tion to a specific audience.

10 (ii) OTHER LIMITATIONS.—The term
11 “publicly available information” does not
12 include—

13 (I) any obscene visual depiction
14 (as defined in section 1460 of title 18,
15 United States Code);

16 (II) any inference made exclu-
17 sively from multiple independent
18 sources of publicly available informa-
19 tion that reveals sensitive covered
20 data with respect to an individual;

21 (III) biometric information;

22 (IV) publicly available informa-
23 tion that has been combined with cov-
24 ered data;

1 (V) genetic information, unless
2 otherwise made available by the indi-
3 vidual to whom the information per-
4 tains as described in clause (ii) or (iii)
5 of subparagraph (A); or

6 (VI) intimate images known to be
7 nonconsensual.

8 (28) SENSITIVE COVERED DATA.—

9 (A) IN GENERAL.—The term “sensitive
10 covered data” means the following types of cov-
11 ered data:

12 (i) A government-issued identifier,
13 such as a Social Security number, passport
14 number, or driver’s license number, that is
15 not required by law to be displayed in pub-
16 lic.

17 (ii) Any information that describes or
18 reveals the past, present, or future physical
19 health, mental health, disability, diagnosis,
20 or healthcare condition or treatment of an
21 individual.

22 (iii) A financial account number, debit
23 card number, credit card number, or infor-
24 mation that describes or reveals the income
25 level or bank account balances of an indi-

1 vidual, except that the last four digits of a
2 debit or credit card number shall not be
3 deemed sensitive covered data.

4 (iv) Biometric information.

5 (v) Genetic information.

6 (vi) Precise geolocation information.

7 (vii) An individual's private commu-
8 nications such as voicemails, emails, texts,
9 direct messages, or mail, or information
10 identifying the parties to such communica-
11 tions, voice communications, video commu-
12 nications, and any information that per-
13 tains to the transmission of such commu-
14 nications, including telephone numbers
15 called, telephone numbers from which calls
16 were placed, the time calls were made, call
17 duration, and location information of the
18 parties to the call, unless the covered enti-
19 ty or a service provider acting on behalf of
20 the covered entity is the sender or an in-
21 tended recipient of the communication.
22 Communications are not private for pur-
23 poses of this clause if such communications
24 are made from or to a device provided by
25 an employer to an employee insofar as

1 such employer provides conspicuous notice
2 that such employer may access such com-
3 munications.

4 (viii) Account or device log-in creden-
5 tials, or security or access codes for an ac-
6 count or device.

7 (ix) Information identifying the sexual
8 behavior of an individual in a manner in-
9 consistent with the individual's reasonable
10 expectation regarding the collection, proc-
11 essing, or transfer of such information.

12 (x) Calendar information, address
13 book information, phone or text logs,
14 photos, audio recordings, or videos, main-
15 tained for private use by an individual, re-
16 gardless of whether such information is
17 stored on the individual's device or is ac-
18 cessible from that device and is backed up
19 in a separate location. Such information is
20 not sensitive for purposes of this para-
21 graph if such information is sent from or
22 to a device provided by an employer to an
23 employee insofar as such employer provides
24 conspicuous notice that it may access such
25 information.

1 (xi) A photograph, film, video record-
2 ing, or other similar medium that shows
3 the naked or undergarment-clad private
4 area of an individual.

5 (xii) Information revealing the video
6 content requested or selected by an indi-
7 vidual collected by a covered entity that is
8 not a provider of a service described in sec-
9 tion 102(4). This clause does not include
10 covered data used solely for transfers for
11 independent video measurement.

12 (xiii) Information about an individual
13 when the covered entity or service provider
14 has knowledge that the individual is a cov-
15 ered minor.

16 (xiv) An individual's race, color, eth-
17 nicity, religion, or union membership.

18 (xv) Information identifying an indi-
19 vidual's online activities over time and
20 across third party websites or online serv-
21 ices.

22 (xvi) Any other covered data collected,
23 processed, or transferred for the purpose
24 of identifying the types of covered data
25 listed in clauses (i) through (xv).

1 (B) RULEMAKING.—The Commission may
2 commence a rulemaking pursuant to section
3 553 of title 5, United States Code, to include
4 in the definition of “sensitive covered data” any
5 other type of covered data that may require a
6 similar level of protection as the types of cov-
7 ered data listed in clauses (i) through (xvi) of
8 subparagraph (A) as a result of any new meth-
9 od of collecting, processing, or transferring cov-
10 ered data.

11 (29) SERVICE PROVIDER.—

12 (A) IN GENERAL.—The term “service pro-
13 vider” means a person or entity that—

14 (i) collects, processes, or transfers
15 covered data on behalf of, and at the direc-
16 tion of, a covered entity or a Federal,
17 State, Tribal, territorial, or local govern-
18 ment entity; and

19 (ii) receives covered data from or on
20 behalf of a covered entity or a Federal,
21 State, Tribal, territorial, or local govern-
22 ment entity.

23 (B) TREATMENT WITH RESPECT TO SERV-
24 ICE PROVIDER DATA.—A service provider that
25 receives service provider data from another

1 service provider as permitted under this Act
2 shall be treated as a service provider under this
3 Act with respect to such data.

4 (30) SERVICE PROVIDER DATA.—The term
5 “service provider data” means covered data that is
6 collected or processed by or has been transferred to
7 a service provider by or on behalf of a covered enti-
8 ty, a Federal, State, Tribal, territorial, or local gov-
9 ernment entity, or another service provider for the
10 purpose of allowing the service provider to whom
11 such covered data is transferred to perform a service
12 or function on behalf of, and at the direction of,
13 such covered entity or Federal, State, Tribal, terri-
14 torial, or local government entity.

15 (31) STATE.—The term “State” means any of
16 the 50 States, the District of Columbia, the Com-
17 monwealth of Puerto Rico, the Virgin Islands of the
18 United States, Guam, American Samoa, or the Com-
19 monwealth of the Northern Mariana Islands.

20 (32) STATE PRIVACY AUTHORITY.—The term
21 “State privacy authority” means—

22 (A) the chief consumer protection officer of
23 a State; or

1 (B) a State consumer protection agency
2 with expertise in data protection, including the
3 California Privacy Protection Agency.

4 (33) SUBSTANTIAL PRIVACY RISK.—The term
5 “substantial privacy risk” means the collection,
6 processing, or transfer of covered data in a manner
7 that may result in any reasonably foreseeable sub-
8 stantial physical injury, economic injury, highly of-
9 fensive intrusion into the privacy expectations of a
10 reasonable individual under the circumstances, or
11 discrimination on the basis of race, color, religion,
12 national origin, sex, or disability.

13 (34) TARGETED ADVERTISING.—The term “tar-
14 geted advertising”—

15 (A) means presenting to an individual or
16 device identified by a unique identifier, or
17 groups of individuals or devices identified by
18 unique identifiers, an online advertisement that
19 is selected based on known or predicted pref-
20 erences, characteristics, or interests associated
21 with the individual or a device identified by a
22 unique identifier; and

23 (B) does not include—

24 (i) advertising or marketing to an in-
25 dividual or an individual’s device in re-

1 sponse to the individual’s specific request
2 for information or feedback;

3 (ii) contextual advertising, which is
4 when an advertisement is displayed based
5 on the content in which the advertisement
6 appears and does not vary based on who is
7 viewing the advertisement; or

8 (iii) processing covered data solely for
9 measuring or reporting advertising or con-
10 tent, performance, reach, or frequency, in-
11 cluding independent measurement.

12 (35) THIRD PARTY.—The term “third party”—

13 (A) means any person or entity, including
14 a covered entity, that—

15 (i) collects, processes, or transfers
16 covered data that the person or entity did
17 not collect directly from the individual
18 linked or linkable to such covered data;
19 and

20 (ii) is not a service provider with re-
21 spect to such data; and

22 (B) does not include a person or entity
23 that collects covered data from another entity if
24 the 2 entities are related by common ownership
25 or corporate control, but only if a reasonable

1 consumer's reasonable expectation would be
2 that such entities share information.

3 (36) THIRD-PARTY COLLECTING ENTITY.—

4 (A) IN GENERAL.—The term “third-party
5 collecting entity”—

6 (i) means a covered entity whose prin-
7 cipal source of revenue is derived from
8 processing or transferring covered data
9 that the covered entity did not collect di-
10 rectly from the individuals linked or
11 linkable to the covered data; and

12 (ii) does not include a covered entity
13 insofar as such entity processes employee
14 data collected by and received from a third
15 party concerning any individual who is an
16 employee of the third party for the sole
17 purpose of such third party providing ben-
18 efits to the employee.

19 (B) PRINCIPAL SOURCE OF REVENUE DE-
20 FINED.—For purposes of this paragraph, the
21 term “principal source of revenue” means, for
22 the prior 12-month period, either—

23 (i) more than 50 percent of all rev-
24 enue of the covered entity; or

1 (ii) obtaining revenue from processing
2 or transferring the covered data of more
3 than 5,000,000 individuals that the cov-
4 ered entity did not collect directly from the
5 individuals linked or linkable to the cov-
6 ered data.

7 (C) NON-APPLICATION TO SERVICE PRO-
8 VIDERS.—An entity may not be considered to
9 be a third-party collecting entity for purposes of
10 this Act if the entity is acting as a service pro-
11 vider.

12 (37) THIRD PARTY DATA.—The term “third
13 party data” means covered data that has been trans-
14 ferred to a third party.

15 (38) TRANSFER.—The term “transfer” means
16 to disclose, release, disseminate, make available, li-
17 cense, rent, or share covered data orally, in writing,
18 electronically, or by any other means.

19 (39) UNIQUE PERSISTENT IDENTIFIER.—The
20 term “unique identifier”—

21 (A) means an identifier to the extent that
22 such identifier is reasonably linkable to an indi-
23 vidual or device that identifies or is linked or
24 reasonably linkable to 1 or more individuals, in-
25 cluding a device identifier, Internet Protocol ad-

1 dress, cookie, beacon, pixel tag, mobile ad iden-
2 tifier, or similar technology, customer number,
3 unique pseudonym, user alias, telephone num-
4 ber, or other form of persistent or probabilistic
5 identifier that is linked or reasonably linkable
6 to an individual or device; and

7 (B) does not include an identifier assigned
8 by a covered entity for the specific purpose of
9 giving effect to an individual's exercise of af-
10 firmative express consent or opt-outs of the col-
11 lection, processing, and transfer of covered data
12 pursuant to section 204 or otherwise limiting
13 the collection, processing, or transfer of such in-
14 formation.

15 (40) WIDELY DISTRIBUTED MEDIA.—The term
16 “widely distributed media” means information that
17 is available to the general public, including informa-
18 tion from a telephone book or online directory, a tel-
19 evision, internet, or radio program, the news media,
20 or an internet site that is available to the general
21 public on an unrestricted basis, but does not include
22 an obscene visual depiction (as defined in section
23 1460 of title 18, United States Code).

1 **TITLE I—DUTY OF LOYALTY**

2 **SEC. 101. DATA MINIMIZATION.**

3 (a) IN GENERAL.—A covered entity may not collect,
4 process, or transfer covered data unless the collection,
5 processing, or transfer is limited to what is reasonably
6 necessary and proportionate to—

7 (1) provide or maintain a specific product or
8 service requested by the individual to whom the data
9 pertains; or

10 (2) effect a purpose permitted under subsection
11 (b).

12 (b) PERMISSIBLE PURPOSES.—A covered entity may
13 collect, process, or transfer covered data for any of the
14 following purposes if the collection, processing, or transfer
15 is limited to what is reasonably necessary and propor-
16 tionate to such purpose:

17 (1) To initiate, manage, or complete a trans-
18 action or fulfill an order for specific products or
19 services requested by an individual, including any as-
20 sociated routine administrative, operational, and ac-
21 count-servicing activity such as billing, shipping, de-
22 livery, storage, and accounting.

23 (2) With respect to covered data previously col-
24 lected in accordance with this Act, notwithstanding
25 this exception—

1 (A) to process such data as necessary to
2 perform system maintenance or diagnostics;

3 (B) to develop, maintain, repair, or en-
4 hance a product or service for which such data
5 was collected;

6 (C) to conduct internal research or ana-
7 lytics to improve a product or service for which
8 such data was collected;

9 (D) to perform inventory management or
10 reasonable network management;

11 (E) to protect against spam; or

12 (F) to debug or repair errors that impair
13 the functionality of a service or product for
14 which such data was collected.

15 (3) To authenticate users of a product or serv-
16 ice.

17 (4) To fulfill a product or service warranty.

18 (5) To prevent, detect, protect against, or re-
19 spond to a security incident. For purposes of this
20 paragraph, security is defined as network security
21 and physical security and life safety, including an in-
22 trusion or trespass, medical alerts, fire alarms, and
23 access control security.

24 (6) To prevent, detect, protect against, or re-
25 spond to fraud, harassment, or illegal activity. For

1 purposes of this paragraph, the term “illegal activ-
2 ity” means a violation of a Federal, State, or local
3 law punishable as a felony or misdemeanor that can
4 directly harm.

5 (7) To comply with a legal obligation imposed
6 by Federal, Tribal, local, or State law, or to inves-
7 tigate, establish, prepare for, exercise, or defend
8 legal claims involving the covered entity or service
9 provider.

10 (8) To prevent an individual, or group of indi-
11 viduals, from suffering harm where the covered enti-
12 ty or service provider believes in good faith that the
13 individual, or group of individuals, is at risk of
14 death, serious physical injury, or other serious
15 health risk.

16 (9) To effectuate a product recall pursuant to
17 Federal or State law.

18 (10)(A) To conduct a public or peer-reviewed
19 scientific, historical, or statistical research project
20 that—

21 (i) is in the public interest; and

22 (ii) adheres to all relevant laws and regula-
23 tions governing such research.

24 (B) Not later than 18 months after the date of
25 enactment of this Act, the Commission should issue

1 guidelines to help covered entities ensure the privacy
2 of affected users and the security of covered data,
3 particularly as data is being transferred to and
4 stored by researchers. Such guidelines should con-
5 sider risks as they pertain to projects using covered
6 data with special considerations for projects that are
7 exempt under part 46 of title 45, Code of Federal
8 Regulations (or any successor regulation) or are ex-
9 cluded from the criteria for institutional review
10 board review.

11 (11) To deliver a communication that is not an
12 advertisement to an individual, if the communication
13 is reasonably anticipated by the individual within the
14 context of the individual's interactions with the cov-
15 ered entity.

16 (12) To deliver a communication at the direc-
17 tion of an individual between such individual and
18 one or more individuals or entities.

19 (13) To transfer assets to a third party in the
20 context of a merger, acquisition, bankruptcy, or
21 similar transaction when the third party assumes
22 control, in whole or in part, of the covered entity's
23 assets, only if the covered entity, in a reasonable
24 time prior to such transfer, provides each affected
25 individual with—

1 (A) a notice describing such transfer, in-
2 cluding the name of the entity or entities receiv-
3 ing the individual's covered data and their pri-
4 vacy policies as described in section 202; and

5 (B) a reasonable opportunity to withdraw
6 any previously given consents in accordance
7 with the requirements of affirmative express
8 consent under this Act related to the individ-
9 ual's covered data and a reasonable opportunity
10 to request the deletion of the individual's cov-
11 ered data, as described in section 203.

12 (14) To ensure the data security and integrity
13 of covered data, as described in section 208.

14 (15) With respect to covered data previously
15 collected in accordance with this Act, a service pro-
16 vider acting at the direction of a government entity,
17 or a service provided to a government entity by a
18 covered entity, and only insofar as authorized by
19 statute, to prevent, detect, protect against or re-
20 spond to a public safety incident, including trespass,
21 natural disaster, or national security incident. This
22 paragraph does not permit, however, the transfer of
23 covered data for payment or other valuable consider-
24 ation to a government entity.

1 (16) With respect to covered data collected in
2 accordance with this Act, notwithstanding this ex-
3 ception, to process such data as necessary to provide
4 first party advertising or marketing of products or
5 services provided by the covered entity for individ-
6 uals who are not-covered minors.

7 (17) With respect to covered data previously
8 collected in accordance with this Act, notwith-
9 standing this exception and provided such collection,
10 processing, and transferring otherwise complies with
11 the requirements of this Act, including section
12 204(c), to provide targeted advertising.

13 (c) GUIDANCE.—The Commission shall issue guid-
14 ance regarding what is reasonably necessary and propor-
15 tionate to comply with this section. Such guidance shall
16 take into consideration—

17 (1) the size of, and the nature, scope, and com-
18 plexity of the activities engaged in by, the covered
19 entity, including whether the covered entity is a
20 large data holder, nonprofit organization, covered
21 entity meeting the requirements of section 209, third
22 party, or third-party collecting entity;

23 (2) the sensitivity of covered data collected,
24 processed, or transferred by the covered entity;

1 (3) the volume of covered data collected, proc-
2 essed, or transferred by the covered entity; and

3 (4) the number of individuals and devices to
4 which the covered data collected, processed, or trans-
5 ferred by the covered entity relates.

6 (d) **DECEPTIVE MARKETING OF A PRODUCT OR**
7 **SERVICE.**—A covered entity or service provider may not
8 engage in deceptive advertising or marketing with respect
9 to a product or service offered to an individual.

10 (e) **JOURNALISM.**—Nothing in this Act shall be con-
11 strued to limit or diminish First Amendment freedoms
12 guaranteed under the Constitution.

13 **SEC. 102. LOYALTY DUTIES.**

14 Notwithstanding section 101 and unless an exception
15 applies, with respect to covered data, a covered entity or
16 service provider may not—

17 (1) collect, process, or transfer a Social Secu-
18 rity number, except when necessary to facilitate an
19 extension of credit, authentication, fraud and iden-
20 tity fraud detection and prevention, the payment or
21 collection of taxes, the enforcement of a contract be-
22 tween parties, or the prevention, investigation, or
23 prosecution of fraud or illegal activity, or as other-
24 wise required by Federal, State, or local law;

1 (2) collect or process sensitive covered data, ex-
2 cept where such collection or processing is strictly
3 necessary to provide or maintain a specific product
4 or service requested by the individual to whom the
5 covered data pertains, or is strictly necessary to ef-
6 fect a purpose enumerated in paragraphs (1)
7 through (12) and (14) through (15) of section
8 101(b);

9 (3) transfer an individual's sensitive covered
10 data to a third party, unless—

11 (A) the transfer is made pursuant to the
12 affirmative express consent of the individual;

13 (B) the transfer is necessary to comply
14 with a legal obligation imposed by Federal,
15 State, Tribal, or local law, or to establish, exer-
16 cise, or defend legal claims;

17 (C) the transfer is necessary to prevent an
18 individual from imminent injury where the cov-
19 ered entity believes in good faith that the indi-
20 vidual is at risk of death, serious physical in-
21 jury, or serious health risk;

22 (D) with respect to covered data collected
23 in accordance with this Act, notwithstanding
24 this exception, a service provider acting at the
25 direction of a government entity, or a service

1 provided to a government entity by a covered
2 entity, and only insofar as authorized by stat-
3 ute, the transfer is necessary to prevent, detect,
4 protect against or respond to a public safety in-
5 cident including trespass, natural disaster, or
6 national security incident. This paragraph does
7 not permit, however, the transfer of covered
8 data for payment or other valuable consider-
9 ation to a government entity;

10 (E) in the case of the transfer of a pass-
11 word, the transfer is necessary to use a des-
12 ignated password manager or is to a covered
13 entity for the exclusive purpose of identifying
14 passwords that are being re-used across sites or
15 accounts;

16 (F) in the case of the transfer of genetic
17 information, the transfer is necessary to per-
18 form a medical diagnosis or medical treatment
19 specifically requested by an individual, or to
20 conduct medical research in accordance with
21 conditions of section 101(b)(10); or

22 (G) to transfer assets in the manner de-
23 scribed in paragraph (13) of section 101(b); or

24 (4) in the case of a provider of broadcast tele-
25 vision service, cable service, satellite service, stream-

1 ing media service, or other video programming serv-
2 ice described in section 713(h)(2) of the Commu-
3 nications Act of 1934 (47 U.S.C. 613(h)(2)), trans-
4 fer to an unaffiliated third party covered data that
5 reveals the video content or services requested or se-
6 lected by an individual from such service, except
7 with the affirmative express consent of the individual
8 or pursuant to one of the permissible purposes enu-
9 merated in paragraphs (1) through (15) of section
10 101(b).

11 **SEC. 103. PRIVACY BY DESIGN.**

12 (a) POLICIES, PRACTICES, AND PROCEDURES.—A
13 covered entity and a service provider shall establish, imple-
14 ment, and maintain reasonable policies, practices, and pro-
15 cedures that reflect the role of the covered entity or service
16 provider in the collection, processing, and transferring of
17 covered data and that—

18 (1) consider applicable Federal laws, rules, or
19 regulations related to covered data the covered entity
20 or service provider collects, processes, or transfers;

21 (2) identify, assess, and mitigate privacy risks
22 related to covered minors, if applicable;

23 (3) mitigate privacy risks, including substantial
24 privacy risks, related to the products and services of
25 the covered entity or the service provider, including

1 in the design, development, and implementation of
2 such products and services, taking into account the
3 role of the covered entity or service provider and the
4 information available to it; and

5 (4) implement reasonable training and safe-
6 guards within the covered entity and service provider
7 to promote compliance with all privacy laws applica-
8 ble to covered data the covered entity collects, proc-
9 esses, or transfers or covered data the service pro-
10 vider collects, processes, or transfers on behalf of the
11 covered entity and mitigate privacy risks, including
12 substantial privacy risks, taking into account the
13 role of the covered entity or service provider and the
14 information available to it.

15 (b) FACTORS TO CONSIDER.—The policies, practices,
16 and procedures established by a covered entity and a serv-
17 ice provider under subsection (a), shall correspond with,
18 as applicable—

19 (1) the size of the covered entity or the service
20 provider and the nature, scope, and complexity of
21 the activities engaged in by the covered entity or
22 service provider, including whether the covered enti-
23 ty or service provider is a large data holder, non-
24 profit organization, entity meeting the requirements
25 of section 209, third party, or third-party collecting

1 entity, taking into account the role of the covered
2 entity or service provider and the information avail-
3 able to it;

4 (2) the sensitivity of the covered data collected,
5 processed, or transferred by the covered entity or
6 service provider;

7 (3) the volume of covered data collected, proc-
8 essed, or transferred by the covered entity or service
9 provider;

10 (4) the number of individuals and devices to
11 which the covered data collected, processed, or trans-
12 ferred by the covered entity or service provider re-
13 lates; and

14 (5) the cost of implementing such policies, prac-
15 tices, and procedures in relation to the risks and na-
16 ture of the covered data.

17 (c) COMMISSION GUIDANCE.—Not later than 1 year
18 after the date of enactment of this Act, the Commission
19 shall issue guidance as to what constitutes reasonable poli-
20 cies, practices, and procedures as required by this section.
21 The Commission shall consider unique circumstances ap-
22 plicable to nonprofit organizations, to entities meeting the
23 requirements of section 209, and to service providers.

1 **SEC. 104. LOYALTY TO INDIVIDUALS WITH RESPECT TO**
2 **PRICING.**

3 (a) RETALIATION THROUGH SERVICE OR PRICING
4 PROHIBITED.—A covered entity may not retaliate against
5 an individual for exercising any of the rights guaranteed
6 by the Act, or any regulations promulgated under this Act,
7 including denying goods or services, charging different
8 prices or rates for goods or services, or providing a dif-
9 ferent level of quality of goods or services.

10 (b) RULES OF CONSTRUCTION.—Nothing in sub-
11 section (a) may be construed to—

12 (1) prohibit the relation of the price of a service
13 or the level of service provided to an individual to
14 the provision, by the individual, of financial informa-
15 tion that is necessarily collected and processed only
16 for the purpose of initiating, rendering, billing for,
17 or collecting payment for a service or product re-
18 quested by the individual;

19 (2) prohibit a covered entity from offering a dif-
20 ferent price, rate, level, quality or selection of goods
21 or services to an individual, including offering goods
22 or services for no fee, if the offering is in connection
23 with an individual's voluntary participation in a
24 bona fide loyalty program;

25 (3) require a covered entity to provide a bona
26 fide loyalty program that would require the covered

1 entity to collect, process, or transfer covered data
2 that the covered entity otherwise would not collect,
3 process, or transfer;

4 (4) prohibit a covered entity from offering a fi-
5 nancial incentive or other consideration to an indi-
6 vidual for participation in market research;

7 (5) prohibit a covered entity from offering dif-
8 ferent types of pricing or functionalities with respect
9 to a product or service based on an individual's exer-
10 cise of a right under section 203(a)(3); or

11 (6) prohibit a covered entity from declining to
12 provide a product or service insofar as the collection
13 and processing of covered data is strictly necessary
14 for such product or service.

15 (c) BONA FIDE LOYALTY PROGRAM DEFINED.—For
16 purposes of this section, the term “bona fide loyalty pro-
17 gram” includes rewards, premium features, discount or
18 club card programs.

19 **TITLE II—CONSUMER DATA** 20 **RIGHTS**

21 **SEC. 201. CONSUMER AWARENESS.**

22 (a) IN GENERAL.—Not later than 90 days after the
23 date of enactment of this Act, the Commission shall pub-
24 lish, on the public website of the Commission, a webpage
25 that describes each provision, right, obligation, and re-

1 quirement of this Act, listed separately for individuals and
2 for covered entities and service providers, and the rem-
3 edies, exemptions, and protections associated with this
4 Act, in plain and concise language and in an easy-to-un-
5 derstand manner.

6 (b) UPDATES.—The Commission shall update the in-
7 formation published under subsection (a) on a quarterly
8 basis as necessitated by any change in law, regulation,
9 guidance, or judicial decisions.

10 (c) ACCESSIBILITY.—The Commission shall publish
11 the information required to be published under subsection
12 (a) in the ten languages with the most users in the United
13 States, according to the most recent United States Cen-
14 sus.

15 **SEC. 202. TRANSPARENCY.**

16 (a) IN GENERAL.—Each covered entity shall make
17 publicly available, in a clear, conspicuous, not misleading,
18 and easy-to-read and readily accessible manner, a privacy
19 policy that provides a detailed and accurate representation
20 of the data collection, processing, and transfer activities
21 of the covered entity.

22 (b) CONTENT OF PRIVACY POLICY.—A covered entity
23 or service provider shall have a privacy policy that in-
24 cludes, at a minimum, the following:

1 (1) The identity and the contact information
2 of—

3 (A) the covered entity or service provider
4 to which the privacy policy applies (including
5 the covered entity's or service provider's points
6 of contact and generic electronic mail addresses,
7 as applicable for privacy and data security in-
8 quiries); and

9 (B) any other entity within the same cor-
10 porate structure as the covered entity or service
11 provider to which covered data is transferred by
12 the covered entity.

13 (2) The categories of covered data the covered
14 entity or service provider collects or processes.

15 (3) The processing purposes for each category
16 of covered data the covered entity or service provider
17 collects or processes.

18 (4) Whether the covered entity or service pro-
19 vider transfers covered data and, if so, each category
20 of service provider and third party to which the cov-
21 ered entity or service provider transfers covered
22 data, the name of each third-party collecting entity
23 to which the covered entity or service provider trans-
24 fers covered data, and the purposes for which such
25 data is transferred to such categories of service pro-

1 viders and third parties or third-party collecting en-
2 tities, except for a transfer to a governmental entity
3 pursuant to a court order or law that prohibits the
4 covered entity or service provider from disclosing
5 such transfer, except for transfers to governmental
6 entities pursuant to a court order or law that pro-
7 hibits the covered entity from disclosing the transfer.

8 (5) The length of time the covered entity or
9 service provider intends to retain each category of
10 covered data, including sensitive covered data, or, if
11 it is not possible to identify that timeframe, the cri-
12 teria used to determine the length of time the cov-
13 ered entity or service provider intends to retain cat-
14 egories of covered data.

15 (6) A prominent description of how an indi-
16 vidual can exercise the rights described in this Act.

17 (7) A general description of the covered entity's
18 or service provider's data security practices.

19 (8) The effective date of the privacy policy.

20 (9) Whether or not any covered data collected
21 by the covered entity or service provider is trans-
22 ferred to, processed in, stored in, or otherwise acces-
23 sible to the People's Republic of China, Russia, Iran,
24 or North Korea.

1 (c) LANGUAGES.—The privacy policy required under
2 subsection (a) shall be made available to the public in each
3 covered language in which the covered entity or service
4 provider—

5 (1) provides a product or service that is subject
6 to the privacy policy; or

7 (2) carries out activities related to such product
8 or service.

9 (d) ACCESSIBILITY.—The covered entity or service
10 provider shall also provide the disclosures under this sec-
11 tion in a manner that is reasonably accessible to and usa-
12 ble by individuals with disabilities.

13 (e) MATERIAL CHANGES.—

14 (1) AFFIRMATIVE EXPRESS CONSENT.—If a
15 covered entity makes a material change to its pri-
16 vacy policy or practices, the covered entity shall no-
17 tify each individual affected by such material change
18 before implementing the material change with re-
19 spect to any prospectively collected covered data and,
20 except as provided in paragraphs (1) through (15)
21 of section 101(b), provide a reasonable opportunity
22 for each individual to withdraw consent to any fur-
23 ther materially different collection, processing, or
24 transfer of previously collected covered data under
25 the changed policy.

1 (2) NOTIFICATION.—The covered entity shall
2 take all reasonable electronic measures to provide di-
3 rect notification regarding material changes to the
4 privacy policy to each affected individual, in each
5 covered language in which the privacy policy is made
6 available, and taking into account available tech-
7 nology and the nature of the relationship.

8 (3) CLARIFICATION.—Nothing in this section
9 may be construed to affect the requirements for cov-
10 ered entities under section 102 or 204.

11 (4) LOG OF MATERIAL CHANGES.—Each large
12 data holder shall retain copies of previous versions
13 of its privacy policy for at least 10 years beginning
14 after the date of enactment of this Act and publish
15 them on its website. Such large data holder shall
16 make publicly available, in a clear, conspicuous, and
17 readily accessible manner, a log describing the date
18 and nature of each material change to its privacy
19 policy over the past 10 years. The descriptions shall
20 be sufficient for a reasonable individual to under-
21 stand the material effect of each material change.
22 The obligations in this paragraph shall not apply to
23 any previous versions of a large data holder's pri-
24 vacy policy, or any material changes to such policy,
25 that precede the date of enactment of this Act.

1 (f) SHORT-FORM NOTICE TO CONSUMERS BY LARGE
2 DATA HOLDERS.—

3 (1) IN GENERAL.—In addition to the privacy
4 policy required under subsection (a), a large data
5 holder that is a covered entity shall provide a short-
6 form notice of its covered data practices in a manner
7 that is—

8 (A) concise, clear, conspicuous, and not
9 misleading;

10 (B) readily accessible to the individual,
11 based on what is reasonably anticipated within
12 the context of the relationship between the indi-
13 vidual and the large data holder;

14 (C) inclusive of an overview of individual
15 rights and disclosures to reasonably draw atten-
16 tion to data practices that may reasonably be
17 unexpected to a reasonable person or that in-
18 volve sensitive covered data; and

19 (D) no more than 500 words in length.

20 (2) RULEMAKING.—The Commission shall issue
21 a rule pursuant to section 553 of title 5, United
22 States Code, establishing the minimum data disclo-
23 sures necessary for the short-form notice required
24 under paragraph (1), which shall not exceed the con-

1 tent requirements in subsection (b) and shall include
2 templates or models of short-form notices.

3 **SEC. 203. INDIVIDUAL DATA OWNERSHIP AND CONTROL.**

4 (a) ACCESS TO, AND CORRECTION, DELETION, AND
5 PORTABILITY OF, COVERED DATA.—In accordance with
6 subsections (b) and (c), a covered entity shall provide an
7 individual, after receiving a verified request from the indi-
8 vidual, with the right to—

9 (1) access—

10 (A) in a human-readable format that a
11 reasonable individual can understand and
12 download from the internet, the covered data
13 (except covered data in a back-up or archival
14 system) of the individual making the request
15 that is collected, processed, or transferred by
16 the covered entity or any service provider of the
17 covered entity within the 24 months preceding
18 the request;

19 (B) the categories of any third party, if ap-
20 plicable, and an option for consumers to obtain
21 the names of any such third party as well as
22 and the categories of any service providers to
23 whom the covered entity has transferred for
24 consideration the covered data of the individual,

1 as well as the categories of sources from which
2 the covered data was collected; and

3 (C) a description of the purpose for which
4 the covered entity transferred the covered data
5 of the individual to a third party or service pro-
6 vider;

7 (2) correct any verifiable substantial inaccuracy
8 or substantially incomplete information with respect
9 to the covered data of the individual that is proc-
10 essed by the covered entity and instruct the covered
11 entity to make reasonable efforts to notify all third
12 parties or service providers to which the covered en-
13 tity transferred such covered data of the corrected
14 information;

15 (3) delete covered data of the individual that is
16 processed by the covered entity and instruct the cov-
17 ered entity to make reasonable efforts to notify all
18 third parties or service provider to which the covered
19 entity transferred such covered data of the individ-
20 ual's deletion request; and

21 (4) to the extent technically feasible, export to
22 the individual or directly to another entity the cov-
23 ered data of the individual that is processed by the
24 covered entity, including inferences linked or reason-
25 ably linkable to the individual but not including

1 other derived data, without licensing restrictions
2 that limit such transfers in—

3 (A) a human-readable format that a rea-
4 sonable individual can understand and
5 download from the internet; and

6 (B) a portable, structured, interoperable,
7 and machine-readable format.

8 (b) INDIVIDUAL AUTONOMY.—A covered entity may
9 not condition, effectively condition, attempt to condition,
10 or attempt to effectively condition the exercise of a right
11 described in subsection (a) through—

12 (1) the use of any false, fictitious, fraudulent,
13 or materially misleading statement or representa-
14 tion; or

15 (2) the design, modification, or manipulation of
16 any user interface with the purpose or substantial
17 effect of obscuring, subverting, or impairing a rea-
18 sonable individual's autonomy, decision making, or
19 choice to exercise such right.

20 (c) TIMING.—

21 (1) IN GENERAL.—Subject to subsections (d)
22 and (e), each request under subsection (a) shall be
23 completed by any—

24 (A) large data holder within 45 days of
25 such request from an individual, unless it is de-

1 monstrably impracticable or impracticably cost-
2 ly to verify such individual;

3 (B) covered entity that is not a large data
4 holder or a covered entity meeting the require-
5 ments of section 209 within 60 days of such re-
6 quest from an individual, unless it is demon-
7 strably impracticable or impracticably costly to
8 verify such individual; or

9 (C) covered entity meeting the require-
10 ments of section 209 within 90 days of such re-
11 quest from an individual, unless it is demon-
12 strably impracticable or impracticably costly to
13 verify such individual.

14 (2) EXTENSION.—A response period set forth
15 in this subsection may be extended once by 45 addi-
16 tional days when reasonably necessary, considering
17 the complexity and number of the individual's re-
18 quests, so long as the covered entity informs the in-
19 dividual of any such extension within the initial 45-
20 day response period, together with the reason for the
21 extension.

22 (d) FREQUENCY AND COST OF ACCESS.—A covered
23 entity—

1 (1) shall provide an individual with the oppor-
2 tunity to exercise each of the rights described in
3 subsection (a); and

4 (2) with respect to—

5 (A) the first 2 times that an individual ex-
6 ercises any right described in subsection (a) in
7 any 12-month period, shall allow the individual
8 to exercise such right free of charge; and

9 (B) any time beyond the initial 2 times de-
10 scribed in subparagraph (A), may allow the in-
11 dividual to exercise such right for a reasonable
12 fee for each request.

13 (e) VERIFICATION AND EXCEPTIONS.—

14 (1) REQUIRED EXCEPTIONS.—A covered entity
15 may not permit an individual to exercise a right de-
16 scribed in subsection (a), in whole or in part, if the
17 covered entity—

18 (A) cannot reasonably verify that the indi-
19 vidual making the request to exercise the right
20 is the individual whose covered data is the sub-
21 ject of the request or an individual authorized
22 to make such a request on the individual's be-
23 half;

1 (B) reasonably believes that the request is
2 made to interfere with a contract between the
3 covered entity and another individual;

4 (C) determines that the exercise of the
5 right would require access to or correction of
6 another individual's sensitive covered data;

7 (D) reasonably believes that the exercise of
8 the right would require the covered entity to en-
9 gage in an unfair or deceptive practice under
10 section 5 of the Federal Trade Commission Act
11 (15 U.S.C. 45); or

12 (E) reasonably believes that the request is
13 made to further fraud, support criminal activ-
14 ity, or the exercise of the right presents a data
15 security threat.

16 (2) ADDITIONAL INFORMATION.—If a covered
17 entity cannot reasonably verify that a request to ex-
18 ercise a right described in subsection (a) is made by
19 the individual whose covered data is the subject of
20 the request (or an individual authorized to make
21 such a request on the individual's behalf), the cov-
22 ered entity—

23 (A) may request that the individual mak-
24 ing the request to exercise the right provide any
25 additional information necessary for the sole

1 purpose of verifying the identity of the indi-
2 vidual; and

3 (B) may not process or transfer such addi-
4 tional information for any other purpose.

5 (3) PERMISSIVE EXCEPTIONS.—

6 (A) IN GENERAL.—A covered entity may
7 decline, with adequate explanation to the indi-
8 vidual, to comply with a request to exercise a
9 right described in subsection (a), in whole or in
10 part, that would—

11 (i) require the covered entity to retain
12 any covered data collected for a single,
13 one-time transaction, if such covered data
14 is not processed or transferred by the cov-
15 ered entity for any purpose other than
16 completing such transaction;

17 (ii) be demonstrably impracticable or
18 prohibitively costly to comply with, and the
19 covered entity shall provide a description
20 to the requestor detailing the inability to
21 comply with the request;

22 (iii) require the covered entity to at-
23 tempt to re-identify de-identified data;

24 (iv) require the covered entity to
25 maintain covered data in an identifiable

1 form or collect, retain, or access any data
2 in order to be capable of associating a
3 verified individual request with covered
4 data of such individual;

5 (v) result in the release of trade se-
6 crets or other privileged or confidential
7 business information;

8 (vi) require the covered entity to cor-
9 rect any covered data that cannot be rea-
10 sonably verified as being inaccurate or in-
11 complete;

12 (vii) interfere with law enforcement,
13 judicial proceedings, investigations, or rea-
14 sonable efforts to guard against, detect,
15 prevent, or investigate fraudulent, mali-
16 cious, or unlawful activity, or enforce valid
17 contracts;

18 (viii) violate Federal or State law or
19 the rights and freedoms of another indi-
20 vidual, including under the Constitution of
21 the United States;

22 (ix) prevent a covered entity from
23 being able to maintain a confidential
24 record of deletion requests, maintained
25 solely for the purpose of preventing cov-

1 ered data of an individual from being
2 recollected after the individual submitted a
3 deletion request and requested that the
4 covered entity no longer collect, process, or
5 transfer such data;

6 (x) fall within an exception enumer-
7 ated in the regulations promulgated by the
8 Commission pursuant to subparagraph
9 (D); or

10 (xi) with respect to requests for dele-
11 tion—

12 (I) unreasonably interfere with
13 the provision of products or services
14 by the covered entity to another per-
15 son it currently serves;

16 (II) delete covered data that re-
17 lates to a public figure and for which
18 the requesting individual has no rea-
19 sonable expectation of privacy;

20 (III) delete covered data reason-
21 ably necessary to perform a contract
22 between the covered entity and the in-
23 dividual;

24 (IV) delete covered data that the
25 covered entity needs to retain in order

1 to comply with professional ethical ob-
2 ligations;

3 (V) delete covered data that the
4 covered entity reasonably believes may
5 be evidence of unlawful activity or an
6 abuse of the covered entity's products
7 or services; or

8 (VI) for private elementary and
9 secondary schools as defined by State
10 law and private institutions of higher
11 education as defined by title I of the
12 Higher Education Act of 1965, delete
13 covered data that would unreasonably
14 interfere with the provision of edu-
15 cation services by or the ordinary op-
16 eration of the school or institution.

17 (B) PARTIAL COMPLIANCE.—In a cir-
18 cumstance that would allow a denial pursuant
19 to subparagraph (A), a covered entity shall par-
20 tially comply with the remainder of the request
21 if it is possible and not unduly burdensome to
22 do so.

23 (C) NUMBER OF REQUESTS.—For pur-
24 poses of subparagraph (A)(ii), the receipt of a
25 large number of verified requests, on its own,

1 may not be considered to render compliance
2 with a request demonstrably impracticable.

3 (D) FURTHER EXCEPTIONS.—The Com-
4 mission may, by regulation as described in sub-
5 section (g), establish additional permissive ex-
6 ceptions necessary to protect the rights of indi-
7 viduals, alleviate undue burdens on covered en-
8 tities, prevent unjust or unreasonable outcomes
9 from the exercise of access, correction, deletion,
10 or portability rights, or as otherwise necessary
11 to fulfill the purposes of this section. In estab-
12 lishing such exceptions, the Commission should
13 consider any relevant changes in technology,
14 means for protecting privacy and other rights,
15 and beneficial uses of covered data by covered
16 entities.

17 (f) LARGE DATA HOLDER METRICS REPORTING.—
18 A large data holder that is a covered entity shall, for each
19 calendar year in which it was a large data holder, do the
20 following:

21 (1) Compile the following metrics for the prior
22 calendar year:

23 (A) The number of verified access requests
24 under subsection (a)(1).

1 (B) The number of verified deletion re-
2 quests under subsection (a)(3).

3 (C) The number of requests to opt-out of
4 covered data transfers under section 204(b).

5 (D) The number of requests to opt-out of
6 targeted advertising under section 204(c).

7 (E) The number of requests in each of
8 subparagraphs (A) through (D) that such large
9 data holder (i) complied with in whole or in
10 part and (ii) denied.

11 (F) The median or mean number of days
12 within which such large data holder sub-
13 stantively responded to the requests in each of
14 subparagraphs (A) through (D).

15 (2) Disclose by July 1 of each applicable cal-
16 endar year the information compiled in paragraph
17 (1) within such large data holder's privacy policy re-
18 quired under section 202 or on the publicly acces-
19 sible website of such large data holder that is acces-
20 sible from a hyperlink included in the privacy policy.

21 (g) REGULATIONS.—Not later than 2 years after the
22 date of enactment of this Act, the Commission shall pro-
23 mulgate regulations, pursuant to section 553 of title 5,
24 United States Code, as necessary to establish processes
25 by which covered entities are to comply with the provisions

1 of this section. Such regulations shall take into consider-
2 ation—

3 (1) the size of, and the nature, scope, and com-
4 plexity of the activities engaged in by the covered en-
5 tity, including whether the covered entity is a large
6 data holder, nonprofit organization, covered entity
7 meeting the requirements of section 209, third
8 party, or third-party collecting entity;

9 (2) the sensitivity of covered data collected,
10 processed, or transferred by the covered entity;

11 (3) the volume of covered data collected, proc-
12 essed, or transferred by the covered entity;

13 (4) the number of individuals and devices to
14 which the covered data collected, processed, or trans-
15 ferred by the covered entity relates; and

16 (5) after consulting the National Institute of
17 Standards and Technology, standards for ensuring
18 the deletion of covered data under this Act where
19 appropriate.

20 (h) ACCESSIBILITY.—A covered entity shall facilitate
21 the ability of individuals to make requests under sub-
22 section (a) in any covered language in which the covered
23 entity provides a product or service. The mechanisms by
24 which a covered entity enables individuals to make re-

1 quests under subsection (a) shall be readily accessible and
2 usable by with individuals with disabilities.

3 **SEC. 204. RIGHT TO CONSENT AND OBJECT.**

4 (a) WITHDRAWAL OF CONSENT.—A covered entity
5 shall provide an individual with a clear and conspicuous,
6 easy-to-execute means to withdraw any affirmative express
7 consent previously provided by the individual that is as
8 easy to execute by a reasonable individual as the means
9 to provide consent, with respect to the processing or trans-
10 fer of the covered data of the individual.

11 (b) RIGHT TO OPT OUT OF COVERED DATA TRANS-
12 FERS.—

13 (1) IN GENERAL.—A covered entity—

14 (A) may not transfer or direct the transfer
15 of the covered data of an individual to a third
16 party if the individual objects to the transfer;
17 and

18 (B) shall allow an individual to object to
19 such a transfer through an opt-out mechanism,
20 as described in section 210.

21 (2) EXCEPTION.—Except as provided in section
22 206(b)(3)(C), a covered entity need not allow an in-
23 dividual to opt out of the collection, processing, or
24 transfer of covered data made pursuant to the ex-

1 ceptions in paragraphs (1) through (15) of section
2 101(b).

3 (c) RIGHT TO OPT OUT OF TARGETED ADVER-
4 TISING.—

5 (1) A covered entity or service provider that di-
6 rectly delivers a targeted advertisement shall—

7 (A) prior to engaging in targeted adver-
8 tising to an individual or device and at all times
9 thereafter, provide such individual with a clear
10 and conspicuous means to opt out of targeted
11 advertising;

12 (B) abide by any opt-out designation by an
13 individual with respect to targeted advertising
14 and notify the covered entity that directed the
15 service provider to deliver the targeted adver-
16 tisement of the opt-out decision; and

17 (C) allow an individual to make an opt-out
18 designation with respect to targeted advertising
19 through an opt-out mechanism, as described in
20 section 210.

21 (2) A covered entity or service provider that re-
22 ceives an opt-out notification pursuant to paragraph
23 (1)(B) or this paragraph shall abide by such opt-out
24 designations by an individual and notify any other
25 person that directed the covered entity or service

1 provider to serve, deliver, or otherwise handle the
2 advertisement of the opt-out decision.

3 (d) INDIVIDUAL AUTONOMY.—A covered entity may
4 not condition, effectively condition, attempt to condition,
5 or attempt to effectively condition the exercise of any indi-
6 vidual right under this section through—

7 (1) the use of any false, fictitious, fraudulent,
8 or materially misleading statement or representa-
9 tion; or

10 (2) the design, modification, or manipulation of
11 any user interface with the purpose or substantial
12 effect of obscuring, subverting, or impairing a rea-
13 sonable individual's autonomy, decision making, or
14 choice to exercise any such right.

15 **SEC. 205. DATA PROTECTIONS FOR CHILDREN AND MI-**
16 **NORS.**

17 (a) PROHIBITION ON TARGETED ADVERTISING TO
18 CHILDREN AND MINORS.—A covered entity may not en-
19 gage in targeted advertising to any individual if the cov-
20 ered entity has knowledge that the individual is a covered
21 minor.

22 (b) DATA TRANSFER REQUIREMENTS RELATED TO
23 COVERED MINORS.—

24 (1) IN GENERAL.—A covered entity may not
25 transfer or direct the transfer of the covered data of

1 a covered minor to a third party if the covered enti-
2 ty—

3 (A) has knowledge that the individual is a
4 covered minor; and

5 (B) has not obtained affirmative express
6 consent from the covered minor or the covered
7 minor’s parent or guardian.

8 (2) EXCEPTION.—A covered entity or service
9 provider may collect, process, or transfer covered
10 data of an individual the covered entity or service
11 provider knows is under the age of 18 solely in order
12 to submit information relating to child victimization
13 to law enforcement or to the nonprofit, national re-
14 source center and clearinghouse congressionally des-
15 ignated to provide assistance to victims, families,
16 child-serving professionals, and the general public on
17 missing and exploited children issues.

18 (c) YOUTH PRIVACY AND MARKETING DIVISION.—

19 (1) ESTABLISHMENT.—There is established
20 within the Commission in the privacy bureau estab-
21 lished in this Act, a division to be known as the
22 “Youth Privacy and Marketing Division” (in this
23 section referred to as the “Division”).

1 (2) DIRECTOR.—The Division shall be headed
2 by a Director, who shall be appointed by the Chair
3 of the Commission.

4 (3) DUTIES.—The Division shall be responsible
5 for assisting the Commission in addressing, as it re-
6 lates to this Act—

7 (A) the privacy of children and minors;
8 and

9 (B) marketing directed at children and mi-
10 nors.

11 (4) STAFF.—The Director of the Division shall
12 hire adequate staff to carry out the duties described
13 in paragraph (3), including by hiring individuals who
14 are experts in data protection, digital advertising,
15 data analytics, and youth development.

16 (5) REPORTS.—Not later than 2 years after the
17 date of enactment of this Act, and annually there-
18 after, the Commission shall submit to the Committee
19 on Commerce, Science, and Transportation of the
20 Senate and the Committee on Energy and Com-
21 merce of the House of Representatives a report that
22 includes—

23 (A) a description of the work of the Divi-
24 sion regarding emerging concerns relating to
25 youth privacy and marketing practices; and

1 (B) an assessment of how effectively the
2 Division has, during the period for which the
3 report is submitted, assisted the Commission to
4 address youth privacy and marketing practices.

5 (6) PUBLICATION.—Not later than 10 days
6 after the date on which a report is submitted under
7 paragraph (5), the Commission shall publish the re-
8 port on its website.

9 (d) REPORT BY THE INSPECTOR GENERAL.—

10 (1) IN GENERAL.—Not later than 2 years after
11 the date of enactment of this Act, and biennially
12 thereafter, the Inspector General of the Commission
13 shall submit to the Commission and to the Com-
14 mittee on Commerce, Science, and Transportation of
15 the Senate and the Committee on Energy and Com-
16 merce of the House of Representatives a report re-
17 garding the safe harbor provisions in section 1304 of
18 the Children’s Online Privacy Protection Act of
19 1998 (15 U.S.C. 6503), which shall include—

20 (A) an analysis of whether the safe harbor
21 provisions are—

22 (i) operating fairly and effectively;

23 and

24 (ii) effectively protecting the interests

25 of children and minors; and

1 (B) any proposal or recommendation for
2 policy changes that would improve the effective-
3 ness of the safe harbor provisions.

4 (2) PUBLICATION.—Not later than 10 days
5 after the date on which a report is submitted under
6 paragraph (1), the Commission shall publish the re-
7 port on the website of the Commission.

8 **SEC. 206. THIRD-PARTY COLLECTING ENTITIES.**

9 (a) NOTICE.—Each third-party collecting entity shall
10 place a clear, conspicuous, not misleading, and readily ac-
11 cessible notice on the website or mobile application of the
12 third-party collecting entity (if the third-party collecting
13 entity maintains such a website or mobile application)
14 that—

15 (1) notifies individuals that the entity is a
16 third-party collecting entity using specific language
17 that the Commission shall develop through rule-
18 making under section 553 of title 5, United States
19 Code;

20 (2) includes a link to the website established
21 under subsection (b)(3); and

22 (3) is reasonably accessible to and usable by in-
23 dividuals with disabilities.

24 (b) THIRD-PARTY COLLECTING ENTITY REGISTRA-
25 TION.—

1 (1) IN GENERAL.—Not later than January 31
2 of each calendar year that follows a calendar year
3 during which a covered entity acted as a third-party
4 collecting entity and processed covered data per-
5 taining to more than 5,000 individuals or devices
6 that identify or are linked or reasonably linkable to
7 an individual, such covered entity shall register with
8 the Commission in accordance with this subsection.

9 (2) REGISTRATION REQUIREMENTS.—In reg-
10 istering with the Commission as required under
11 paragraph (1), a third-party collecting entity shall
12 do the following:

13 (A) Pay to the Commission a registration
14 fee of \$100.

15 (B) Provide the Commission with the fol-
16 lowing information:

17 (i) The legal name and primary phys-
18 ical, email, and internet addresses of the
19 third-party collecting entity.

20 (ii) A description of the categories of
21 covered data the third-party collecting enti-
22 ty processes and transfers.

23 (iii) The contact information of the
24 third-party collecting entity, including a
25 contact person, a telephone number, an e-

1 mail address, a website, and a physical
2 mailing address.

3 (iv) A link to a website through which
4 an individual may easily exercise the rights
5 provided under this subsection.

6 (3) THIRD-PARTY COLLECTING ENTITY REG-
7 ISTRY.—The Commission shall establish and main-
8 tain on a website a searchable, publicly available,
9 central registry of third-party collecting entities that
10 are registered with the Commission under this sub-
11 section that includes the following:

12 (A) A listing of all registered third-party
13 collecting entities and a search feature that al-
14 lows members of the public to identify indi-
15 vidual third-party collecting entities.

16 (B) For each registered third-party col-
17 lecting entity, the information provided under
18 paragraph (2)(B).

19 (C)(i) A “Do Not Collect” registry link
20 and mechanism by which an individual may,
21 easily submit a request to all registered third-
22 party collecting entities that are not consumer
23 reporting agencies (as defined in section 603(f)
24 of the Fair Credit Reporting Act (15 U.S.C.
25 1681a(f))), and to the extent such third-party

1 collecting entities are not acting as consumer
2 reporting agencies (as so defined), to—

3 (I) delete all covered data related to
4 such individual that the third-party col-
5 lecting entity did not collect from such in-
6 dividual directly or when acting as a serv-
7 ice provider; and

8 (II) ensure that the third-party col-
9 lecting entity no longer collects covered
10 data related to such individual without the
11 affirmative express consent of such indi-
12 vidual, except insofar as the third-party
13 collecting entity is acting as a service pro-
14 vider.

15 (ii) Each third-party collecting entity that
16 receives such a request from an individual shall
17 delete all the covered data of the individual not
18 later than 30 days after the request is received
19 by the third-party collecting entity.

20 (iii) Notwithstanding the provisions of
21 clauses (i) and (ii), a third-party collecting enti-
22 ty may decline to fulfill a “Do Not Collect” re-
23 quest from an individual who it has actual
24 knowledge has been convicted of a crime related
25 to the abduction or sexual exploitation of a

1 child, and the data the entity is collecting is
2 necessary to effectuate the purposes of a na-
3 tional or State-run sex offender registry or the
4 congressionally designated entity that serves as
5 the nonprofit national resource center and
6 clearinghouse to provide assistance to victims,
7 families, child-serving professionals, and the
8 general public on missing and exploited children
9 issues.

10 (c) PENALTIES.—

11 (1) IN GENERAL.—A third-party collecting enti-
12 ty that fails to register or provide the notice as re-
13 quired under this section shall be liable for—

14 (A) a civil penalty of \$100 for each day
15 the third-party collecting entity fails to register
16 or provide notice as required under this section,
17 not to exceed a total of \$10,000 for any year;
18 and

19 (B) an amount equal to the registration
20 fees due under paragraph (2)(A) of subsection
21 (b) for each year that the third-party collecting
22 entity failed to register as required under para-
23 graph (1) of such subsection.

24 (2) RULE OF CONSTRUCTION.—Nothing in this
25 subsection shall be construed as altering, limiting, or

1 affecting any enforcement authorities or remedies
2 under this Act.

3 **SEC. 207. CIVIL RIGHTS AND ALGORITHMS.**

4 (a) CIVIL RIGHTS PROTECTIONS.—

5 (1) IN GENERAL.—A covered entity or a service
6 provider may not collect, process, or transfer covered
7 data in a manner that discriminates in or otherwise
8 makes unavailable the equal enjoyment of goods or
9 services on the basis of race, color, religion, national
10 origin, sex, or disability.

11 (2) EXCEPTIONS.—This subsection shall not
12 apply to—

13 (A) the collection, processing, or transfer
14 of covered data for the purpose of—

15 (i) a covered entity's or a service pro-
16 vider's self-testing to prevent or mitigate
17 unlawful discrimination; or

18 (ii) diversifying an applicant, partici-
19 pant, or customer pool; or

20 (B) any private club or group not open to
21 the public, as described in section 201(e) of the
22 Civil Rights Act of 1964 (42 U.S.C. 2000a(e)).

23 (b) FTC ENFORCEMENT ASSISTANCE.—

24 (1) IN GENERAL.—Whenever the Commission
25 obtains information that a covered entity or service

1 provider may have collected, processed, or trans-
2 ferred covered data in violation of subsection (a), the
3 Commission shall transmit such information as al-
4 lowable under Federal law to any Executive agency
5 with authority to initiate enforcement actions or pro-
6 ceedings relating to such violation.

7 (2) ANNUAL REPORT.—Not later than 3 years
8 after the date of enactment of this Act, and annually
9 thereafter, the Commission shall submit to Congress
10 a report that includes a summary of—

11 (A) the types of information the Commis-
12 sion transmitted to Executive agencies under
13 paragraph (1) during the previous 1-year pe-
14 riod; and

15 (B) how such information relates to Fed-
16 eral civil rights laws.

17 (3) TECHNICAL ASSISTANCE.—In transmitting
18 information under paragraph (1), the Commission
19 may consult and coordinate with, and provide tech-
20 nical and investigative assistance, as appropriate, to
21 such Executive agency.

22 (4) COOPERATION WITH OTHER AGENCIES.—
23 The Commission may implement this subsection by
24 executing agreements or memoranda of under-
25 standing with the appropriate Executive agencies.

1 (c) COVERED ALGORITHM IMPACT AND EVALUA-
2 TION.—

3 (1) COVERED ALGORITHM IMPACT ASSESS-
4 MENT.—

5 (A) IMPACT ASSESSMENT.—Notwith-
6 standing any other provision of law, not later
7 than 2 years after the date of enactment of this
8 Act, and annually thereafter, a large data hold-
9 er that uses a covered algorithm in a manner
10 that poses a consequential risk of harm to an
11 individual or group of individuals, and uses
12 such covered algorithm solely or in part, to col-
13 lect, process, or transfer covered data shall con-
14 duct an impact assessment of such algorithm in
15 accordance with subparagraph (B).

16 (B) IMPACT ASSESSMENT SCOPE.—The im-
17 pact assessment required under subparagraph
18 (A) shall provide the following:

19 (i) A detailed description of the design
20 process and methodologies of the covered
21 algorithm.

22 (ii) A statement of the purpose and
23 proposed uses of the covered algorithm.

24 (iii) A detailed description of the data
25 used by the covered algorithm, including

1 the specific categories of data that will be
2 processed as input and any data used to
3 train the model that the covered algorithm
4 relies on, if applicable.

5 (iv) A description of the outputs pro-
6 duced by the covered algorithm.

7 (v) An assessment of the necessity
8 and proportionality of the covered algo-
9 rithm in relation to its stated purpose.

10 (vi) A detailed description of steps the
11 large data holder has taken or will take to
12 mitigate potential harms from the covered
13 algorithm to an individual or group of indi-
14 viduals, including related to—

15 (I) covered minors;

16 (II) making or facilitating adver-
17 tising for, or determining access to, or
18 restrictions on the use of housing,
19 education, employment, healthcare, in-
20 surance, or credit opportunities;

21 (III) determining access to, or re-
22 strictions on the use of, any place of
23 public accommodation, particularly as
24 such harms relate to the protected
25 characteristics of individuals, includ-

1 ing race, color, religion, national ori-
2 gin, sex, or disability;

3 (IV) disparate impact on the
4 basis of individuals' race, color, reli-
5 gion, national origin, sex, or disability
6 status; or

7 (V) disparate impact on the basis
8 of individuals' political party registra-
9 tion status.

10 (2) ALGORITHM DESIGN EVALUATION.—Not-
11 withstanding any other provision of law, not later
12 than 2 years after the date of enactment of this Act,
13 a covered entity or service provider that knowingly
14 develops a covered algorithm that is designed to,
15 solely or in part, to collect, process, or transfer cov-
16 ered data in furtherance of a consequential decision
17 shall prior to deploying the covered algorithm in
18 interstate commerce evaluate the design, structure,
19 and inputs of the covered algorithm, including any
20 training data used to develop the covered algorithm,
21 to reduce the risk of the potential harms identified
22 under paragraph (1)(B).

23 (3) OTHER CONSIDERATIONS.—

24 (A) FOCUS.—In complying with para-
25 graphs (1) and (2), a covered entity and a serv-

1 ice provider may focus the impact assessment
2 or evaluation on any covered algorithm, or por-
3 tions of a covered algorithm, that will be put to
4 use and may reasonably contribute to the risk
5 of the potential harms identified under para-
6 graph (1)(B).

7 (B) AVAILABILITY.—

8 (i) IN GENERAL.—A covered entity
9 and a service provider—

10 (I) shall, not later than 30 days
11 after completing an impact assess-
12 ment or evaluation, submit the impact
13 assessment or evaluation conducted
14 under paragraph (1) or (2) to the
15 Commission;

16 (II) shall, upon request, make
17 such impact assessment and evalua-
18 tion available to Congress; and

19 (III) may make a summary of
20 such impact assessment and evalua-
21 tion publicly available in a place that
22 is easily accessible to individuals.

23 (ii) TRADE SECRETS.—Covered enti-
24 ties and service providers may redact and
25 segregate any trade secret (as defined in

1 section 1839 of title 18, United States
2 Code) or other confidential or proprietary
3 information from public disclosure under
4 this subparagraph and the Commission
5 shall abide by its obligations under section
6 6(f) of the Federal Trade Commission Act
7 (15 U.S.C. 46(f)) in regard to such infor-
8 mation.

9 (C) ENFORCEMENT.—The Commission
10 may not use any information obtained solely
11 and exclusively through a covered entity or a
12 service provider's disclosure of information to
13 the Commission in compliance with this section
14 for any purpose other than enforcing this Act
15 with the exception of enforcing consent orders,
16 including the study and report provisions in
17 paragraph (6). This subparagraph does not pre-
18 clude the Commission from providing this infor-
19 mation to Congress in response to a subpoena.

20 (4) GUIDANCE.—Not later than 2 years after
21 the date of enactment of this Act, the Commission
22 shall, in consultation with the Secretary of Com-
23 merce, or their respective designees, publish guid-
24 ance regarding compliance with this section.

1 (5) RULEMAKING AND EXEMPTION.—The Com-
2 mission shall have authority under section 553 of
3 title 5, United States Code, to promulgate regula-
4 tions as necessary to establish processes by which a
5 large data holder—

6 (A) shall submit an impact assessment to
7 the Commission under paragraph (3)(B)(i)(I);
8 and

9 (B) may exclude from this subsection any
10 covered algorithm that presents low or minimal
11 consequential risk of harm to an individual or
12 group of individuals.

13 (6) STUDY AND REPORT.—

14 (A) STUDY.—The Commission, in con-
15 sultation with the Secretary of Commerce or
16 the Secretary's designee, shall conduct a study,
17 to review any impact assessment or evaluation
18 submitted under this subsection. Such study
19 shall include an examination of—

20 (i) best practices for the assessment
21 and evaluation of covered algorithms; and

22 (ii) methods to reduce the risk of
23 harm to individuals that may be related to
24 the use of covered algorithms.

25 (B) REPORT.—

1 (i) INITIAL REPORT.—Not later than
2 3 years after the date of enactment of this
3 Act, the Commission, in consultation with
4 the Secretary of Commerce or the Sec-
5 retary’s designee, shall submit to Congress
6 a report containing the results of the study
7 conducted under subparagraph (A), to-
8 gether with recommendations for such leg-
9 islation and administrative action as the
10 Commission determines appropriate.

11 (ii) ADDITIONAL REPORTS.—Not later
12 than 3 years after submission of the initial
13 report under clause (i), and as the Com-
14 mission determines necessary thereafter,
15 the Commission shall submit to Congress
16 an updated version of such report.

17 **SEC. 208. DATA SECURITY AND PROTECTION OF COVERED**
18 **DATA.**

19 (a) ESTABLISHMENT OF DATA SECURITY PRAC-
20 TICES.—

21 (1) IN GENERAL.—A covered entity or service
22 provider shall establish, implement, and maintain
23 reasonable administrative, technical, and physical
24 data security practices and procedures to protect

1 and secure covered data against unauthorized access
2 and acquisition.

3 (2) CONSIDERATIONS.—The reasonable admin-
4 istrative, technical, and physical data security prac-
5 tices required under paragraph (1) shall be appro-
6 priate to—

7 (A) the size and complexity of the covered
8 entity or service provider;

9 (B) the nature and scope of the covered
10 entity or the service provider's collecting, proc-
11 essing, or transferring of covered data;

12 (C) the volume and nature of the covered
13 data collected, processed, or transferred by the
14 covered entity or service provider;

15 (D) the sensitivity of the covered data col-
16 lected, processed, or transferred;

17 (E) the current state of the art (and limi-
18 tations thereof) in administrative, technical,
19 and physical safeguards for protecting such cov-
20 ered data; and

21 (F) the cost of available tools to improve
22 security and reduce vulnerabilities to unauthor-
23 ized access and acquisition of such covered data
24 in relation to the risks and nature of the cov-
25 ered data.

1 (b) SPECIFIC REQUIREMENTS.—The data security
2 practices of the covered entity and of the service provider
3 required under subsection (a) shall include, for each re-
4 spective entity's own system or systems, at a minimum,
5 the following practices:

6 (1) ASSESS VULNERABILITIES.—Identifying
7 and assessing any material internal and external
8 risk to, and vulnerability in, the security of each sys-
9 tem maintained by the covered entity that collects,
10 processes, or transfers covered data, or service pro-
11 vider that collects, processes, or transfers covered
12 data on behalf of the covered entity, including unau-
13 thorized access to or risks to such covered data,
14 human vulnerabilities, access rights, and the use of
15 service providers. With respect to large data holders,
16 such activities shall include a plan to receive and
17 reasonably respond to unsolicited reports of
18 vulnerabilities by any entity or individual and by
19 performing a reasonable investigation of such re-
20 ports.

21 (2) PREVENTIVE AND CORRECTIVE ACTION.—
22 Taking preventive and corrective action designed to
23 mitigate reasonably foreseeable risks or
24 vulnerabilities to covered data identified by the cov-
25 ered entity or service provider, consistent with the

1 nature of such risk or vulnerability and the entity's
2 role in collecting, processing, or transferring the
3 data. Such action may include implementing admin-
4 istrative, technical, or physical safeguards or
5 changes to data security practices or the architec-
6 ture, installation, or implementation of network or
7 operating software, among other actions.

8 (3) EVALUATION OF PREVENTIVE AND CORREC-
9 TIVE ACTION.—Evaluating and making reasonable
10 adjustments to the action described in paragraph (2)
11 in light of any material changes in technology, inter-
12 nal or external threats to covered data, and the cov-
13 ered entity or service provider's own changing busi-
14 ness arrangements or operations.

15 (4) INFORMATION RETENTION AND DIS-
16 POSAL.—Disposing of covered data in accordance
17 with a retention schedule that shall require the dele-
18 tion of covered data when such data is required to
19 be deleted by law or is no longer necessary for the
20 purpose for which the data was collected, processed,
21 or transferred, unless an individual has provided af-
22 firmative express consent to such retention. Such
23 disposal shall include destroying, permanently eras-
24 ing, or otherwise modifying the covered data to
25 make such data permanently unreadable or indeci-

1 pherable and unrecoverable to ensure ongoing com-
2 pliance with this section. Service providers shall es-
3 tablish practices to delete or return covered data to
4 a covered entity as requested at the end of the provi-
5 sion of services unless retention of the covered data
6 is required by law, consistent with section 302(a)(6).

7 (5) TRAINING.—Training each employee with
8 access to covered data on how to safeguard covered
9 data and updating such training as necessary.

10 (6) DESIGNATION.—Designating an officer, em-
11 ployee, or employees to maintain and implement
12 such practices.

13 (7) INCIDENT RESPONSE.—Implementing pro-
14 cedures to detect, respond to, or recover from secu-
15 rity incidents, including breaches.

16 **SEC. 209. SMALL BUSINESS PROTECTIONS.**

17 (a) ESTABLISHMENT OF EXEMPTION.—Any covered
18 entity or service provider that can establish that it met
19 the requirements described in subsection (b) for the period
20 of the 3 preceding calendar years (or for the period during
21 which the covered entity or service provider has been in
22 existence if such period is less than 3 years) shall—

23 (1) be exempt from compliance with section
24 203(a)(4) and paragraphs (1) through (3) and (5)
25 through (7) of section 208(b); and

1 (2) at the covered entity's sole discretion, have
2 the option of complying with section 203(a)(2) by,
3 after receiving a verified request from an individual
4 to correct covered data of the individual under such
5 section, deleting such covered data in its entirety in-
6 stead of making the requested correction.

7 (b) EXEMPTION REQUIREMENTS.—The requirements
8 of this subsection are, with respect to a covered entity or
9 a service provider, the following:

10 (1) The covered entity or service provider's av-
11 erage annual gross revenues during the period did
12 not exceed \$41,000,000.

13 (2) The covered entity or service provider, on
14 average, did not annually collect or process the cov-
15 ered data of more than 200,000 individuals during
16 the period beyond the purpose of initiating, ren-
17 dering, billing for, finalizing, completing, or other-
18 wise collecting payment for a requested service or
19 product, so long as all covered data for such purpose
20 was deleted or de-identified within 90 days, except
21 when necessary to investigate fraud or as consistent
22 with a covered entity's return policy.

23 (3) The covered entity or service provider did
24 not derive more than 50 percent of its revenue from
25 transferring covered data during any year (or part

1 of a year if the covered entity has been in existence
2 for less than 1 year) that occurs during the period.

3 (c) REVENUE DEFINED.—For purposes of this sec-
4 tion, the term “revenue” as it relates to any covered entity
5 or service provider that is not organized to carry on busi-
6 ness for its own profit or that of its members, means the
7 gross receipts the covered entity or service provider re-
8 ceived in whatever form from all sources without sub-
9 tracting any costs or expenses, and includes contributions,
10 gifts, grants, dues or other assessments, income from in-
11 vestments, or proceeds from the sale of real or personal
12 property.

13 **SEC. 210. UNIFIED OPT-OUT MECHANISMS.**

14 (a) IN GENERAL.—For the rights established under
15 subsection (b) of section 204, subsection (c) of section 204
16 (except as provided for under section 101(b)(16)), and
17 section 206(b)(3)(C), following public notice and oppor-
18 tunity to comment and not later than 18 months after
19 the date of enactment of this Act, the Commission shall
20 establish or recognize one or more acceptable privacy pro-
21 tective, centralized mechanisms, including global privacy
22 signals such as browser or device privacy settings, other
23 tools offered by covered entities or service providers, and
24 registries of identifiers, for individuals to exercise all such
25 rights through a single interface for a covered entity or

1 service provider to utilize to allow an individual to make
2 such opt out designations with respect to covered data re-
3 lated to such individual.

4 (b) REQUIREMENTS.—Any such centralized opt-out
5 mechanism shall—

6 (1) require covered entities or service providers
7 acting on behalf of covered entities to inform indi-
8 viduals about the centralized opt-out choice;

9 (2) not be required to be the default setting,
10 but may be the default setting provided that in all
11 cases the mechanism clearly represents the individ-
12 ual's affirmative, freely given, and unambiguous
13 choice to opt out;

14 (3) be consumer-friendly, clearly described, and
15 easy-to-use by a reasonable individual;

16 (4) permit the covered entity or service provider
17 acting on behalf of a covered entity to have an au-
18 thentication process the covered entity or service
19 provider acting on behalf of a covered entity may
20 use to determine if the mechanism represents a le-
21 gitimate request to opt out;

22 (5) be provided in any covered language in
23 which the covered entity provides products or serv-
24 ices subject to the opt-out; and

1 (6) be provided in a manner that is reasonably
2 accessible to and usable by individuals with disabil-
3 ities.

4 **TITLE III—CORPORATE** 5 **ACCOUNTABILITY**

6 **SEC. 301. EXECUTIVE RESPONSIBILITY.**

7 (a) IN GENERAL.—Beginning 1 year after the date
8 of enactment of this Act, an executive officer of a large
9 data holder shall annually certify, in good faith, to the
10 Commission, in a manner specified by the Commission by
11 regulation under section 553 of title 5, United States
12 Code, that the entity maintains—

13 (1) internal controls reasonably designed to
14 comply with this Act; and

15 (2) internal reporting structures to ensure that
16 such certifying executive officer is involved in and
17 responsible for the decisions that impact the compli-
18 ance by the large data holder with this Act.

19 (b) REQUIREMENTS.—A certification submitted
20 under subsection (a) shall be based on a review of the ef-
21 fectiveness of the internal controls and reporting struc-
22 tures of the large data holder that is conducted by the
23 certifying executive officer not more than 90 days before
24 the submission of the certification. A certification sub-
25 mitted under subsection (a) is made in good faith if the

1 certifying officer had, after a reasonable investigation, rea-
2 sonable ground to believe and did believe, at the time that
3 certification was submitted, that the statements therein
4 were true and that there was no omission to state a mate-
5 rial fact required to be stated therein or necessary to make
6 the statements therein not misleading.

7 (c) LARGE DATA HOLDER PRIVACY IMPACT ASSESS-
8 MENTS.—

9 (1) IN GENERAL.—Not later than 1 year after
10 the date of enactment of this Act or 1 year after the
11 date on which a covered entity first meets the defini-
12 tion of large data holder, whichever is earlier, and
13 biennially thereafter, each covered entity that is a
14 large data holder shall conduct a privacy impact as-
15 sessment that weighs the benefits of the large data
16 holder's covered data collecting, processing, and
17 transfer practices against the potential adverse con-
18 sequences of such practices, including substantial
19 privacy risks, to individual privacy.

20 (2) ASSESSMENT REQUIREMENTS.—A privacy
21 impact assessment required under paragraph (1)
22 shall be—

23 (A) reasonable and appropriate in scope
24 given—

1 (i) the nature of the covered data col-
2 lected, processed, and transferred by the
3 large data holder;

4 (ii) the volume of the covered data
5 collected, processed, and transferred by the
6 large data holder; and

7 (iii) the potential material risks posed
8 to the privacy of individuals by the col-
9 lecting, processing, and transfer of covered
10 data by the large data holder; and

11 (B) documented in written form and main-
12 tained by the large data holder unless rendered
13 out of date by a subsequent assessment con-
14 ducted under paragraph (1).

15 (3) ADDITIONAL FACTORS TO INCLUDE IN AS-
16 SESSMENT.—In assessing the privacy risks, includ-
17 ing substantial privacy risks, the large data holder
18 must include reviews of the means by which tech-
19 nologies, including blockchain and distributed ledger
20 technologies and other emerging technologies, are
21 used to secure covered data.

22 (d) OTHER PRIVACY IMPACT ASSESSMENTS.—

23 (1) IN GENERAL.—Not later than 1 year after
24 the date of enactment of this Act and biennially
25 thereafter, each covered entity that is not large data

1 holder and does not meet the requirements for cov-
2 ered entities under section 209 shall conduct a pri-
3 vacy impact assessment. Such assessment shall
4 weigh the benefits of the covered entity's covered
5 data collecting, processing, and transfer practices
6 that may cause a substantial privacy risk against the
7 potential material adverse consequences of such
8 practices to individual privacy.

9 (2) ASSESSMENT REQUIREMENTS.—A privacy
10 impact assessment required under paragraph (1)
11 shall be—

12 (A) reasonable and appropriate in scope
13 given—

14 (i) the nature of the covered data col-
15 lected, processed, and transferred by the
16 covered entity;

17 (ii) the volume of the covered data
18 collected, processed, and transferred by the
19 covered entity; and

20 (iii) the potential risks posed to the
21 privacy of individuals by the collecting,
22 processing, and transfer of covered data by
23 the covered entity; and

24 (B) documented in written form and main-
25 tained by the covered entity unless rendered out

1 of date by a subsequent assessment conducted
2 under paragraph (1).

3 (3) ADDITIONAL FACTORS TO INCLUDE IN AS-
4 SESSMENT.—In assessing the privacy risks, includ-
5 ing substantial privacy risks, the covered entity may
6 include reviews of the means by which technologies,
7 including blockchain and distributed ledger tech-
8 nologies and other emerging technologies, are used
9 to secure covered data.

10 **SEC. 302. TECHNICAL COMPLIANCE PROGRAMS.**

11 (a) IN GENERAL.—Not later than 3 years after the
12 date of enactment of this Act, the Commission shall pro-
13 mulgate regulations under section 553 of title 5, United
14 States Code, to establish a process for the proposal and
15 approval of technical compliance programs under this sec-
16 tion used by a covered entity to collect, process, or transfer
17 covered data.

18 (b) SCOPE OF PROGRAMS.—The technical compliance
19 programs established under this section shall, with respect
20 to a technology, product, service, or method used by a cov-
21 ered entity to collect, process, or transfer covered data—

22 (1) establish publicly available guidelines for
23 compliance with this Act; and

24 (2) meet or exceed the requirements of this Act.

25 (c) APPROVAL PROCESS.—

1 (1) IN GENERAL.—Any request for approval,
2 amendment, or repeal of a technical compliance pro-
3 gram may be submitted to the Commission by any
4 person, including a covered entity, a representative
5 of a covered entity, an association of covered enti-
6 ties, or a public interest group or organization.
7 Within 90 days after the request is made, the Com-
8 mission shall publish the request and provide an op-
9 portunity for public comment on the proposal.

10 (2) EXPEDITED RESPONSE TO REQUESTS.—Be-
11 ginning 1 year after the date of enactment of this
12 Act, the Commission shall act upon a request for the
13 proposal and approval of a technical compliance pro-
14 gram not later than 1 year after the filing of the re-
15 quest, and shall set forth publicly in writing the con-
16 clusions of the Commission with regard to such re-
17 quest.

18 (d) RIGHT TO APPEAL.—Final action by the Com-
19 mission on a request for approval, amendment, or repeal
20 of a technical compliance program, or the failure to act
21 within the 1-year period after a request for approval,
22 amendment, or repeal of a technical compliance program
23 is made under subsection (c), may be appealed to a Fed-
24 eral district court of the United States of appropriate ju-

1 jurisdiction as provided for in section 702 of title 5, United
2 States Code.

3 (e) EFFECT ON ENFORCEMENT.—

4 (1) IN GENERAL.—Prior to commencing an in-
5 vestigation or enforcement action against any cov-
6 ered entity under this Act, the Commission and
7 State attorney general shall consider the covered en-
8 tity's history of compliance with any technical com-
9 pliance program approved under this section and
10 any action taken by the covered entity to remedy
11 noncompliance with such program. If such enforce-
12 ment action described in section 403 is brought, the
13 covered entity's history of compliance with any tech-
14 nical compliance program approved under this sec-
15 tion and any action taken by the covered entity to
16 remedy noncompliance with such program shall be
17 taken into consideration when determining liability
18 or a penalty. The covered entity's history of compli-
19 ance with any technical compliance program shall
20 not affect any burden of proof or the weight given
21 to evidence in an enforcement or judicial proceeding.

22 (2) COMMISSION AUTHORITY.—Approval of a
23 technical compliance program shall not limit the au-
24 thority of the Commission, including the Commis-
25 sion's authority to commence an investigation or en-

1 enforcement action against any covered entity under
2 this Act or any other Act.

3 (3) RULE OF CONSTRUCTION.—Nothing in this
4 subsection shall provide any individual, class of indi-
5 viduals, or person with any right to seek discovery
6 of any non-public Commission deliberation or activ-
7 ity or impose any pleading requirement on the Com-
8 mission if the Commission brings an enforcement ac-
9 tion of any kind.

10 **SEC. 303. COMMISSION APPROVED COMPLIANCE GUIDE-**
11 **LINES.**

12 (a) APPLICATION FOR COMPLIANCE GUIDELINE AP-
13 PROVAL.—

14 (1) IN GENERAL.—A covered entity that is not
15 a third-party collecting entity and meets the require-
16 ments of section 209, or a group of such covered en-
17 tities, may apply to the Commission for approval of
18 1 or more sets of compliance guidelines governing
19 the collection, processing, and transfer of covered
20 data by the covered entity or group of covered enti-
21 ties.

22 (2) APPLICATION REQUIREMENTS.—Such appli-
23 cation shall include—

1 (A) a description of how the proposed
2 guidelines will meet or exceed the requirements
3 of this Act;

4 (B) a description of the entities or activi-
5 ties the proposed set of compliance guidelines is
6 designed to cover;

7 (C) a list of the covered entities that meet
8 the requirements of section 209 and are not
9 third-party collecting entities, if any are known
10 at the time of application, that intend to adhere
11 to the compliance guidelines; and

12 (D) a description of how such covered enti-
13 ties will be independently assessed for adher-
14 ence to such compliance guidelines, including
15 the independent organization not associated
16 with any of the covered entities that may par-
17 ticipate in guidelines that will administer such
18 guidelines.

19 (3) COMMISSION REVIEW.—

20 (A) INITIAL APPROVAL.—

21 (i) PUBLIC COMMENT PERIOD.—With-
22 in 90 days after the receipt of proposed
23 guidelines submitted pursuant to para-
24 graph (2), the Commission shall publish
25 the application and provide an opportunity

1 for public comment on such compliance
2 guidelines.

3 (ii) APPROVAL.—The Commission
4 shall approve an application regarding pro-
5 posed guidelines under paragraph (2) if
6 the applicant demonstrates that the com-
7 pliance guidelines—

8 (I) meet or exceed requirements
9 of this Act;

10 (II) provide for the regular re-
11 view and validation by an independent
12 organization not associated with any
13 of the covered entities that may par-
14 ticipate in the guidelines and that is
15 approved by the Commission to con-
16 duct such reviews of the compliance
17 guidelines of the covered entity or en-
18 tities to ensure that the covered entity
19 or entities continue to meet or exceed
20 the requirements of this Act; and

21 (III) include a means of enforce-
22 ment if a covered entity does not meet
23 or exceed the requirements in the
24 guidelines, which may include referral
25 to the Commission for enforcement

1 consistent with section 401 or referral
2 to the appropriate State attorney gen-
3 eral for enforcement consistent with
4 section 402.

5 (iii) **TIMELINE.**—Within 1 year after
6 receiving an application regarding pro-
7 posed guidelines under paragraph (2), the
8 Commission shall issue a determination ap-
9 proving or denying the application and
10 providing its reasons for approving or de-
11 nying such application.

12 (B) **APPROVAL OF MODIFICATIONS.**—

13 (i) **IN GENERAL.**—If the independent
14 organization administering a set of guide-
15 lines makes material changes to guidelines
16 previously approved by the Commission,
17 the independent organization shall submit
18 the updated guidelines to the Commission
19 for approval. As soon as feasible, the Com-
20 mission shall publish the updated guide-
21 lines and provide an opportunity for public
22 comment.

23 (ii) **TIMELINE.**—The Commission
24 shall approve or deny any material change

1 to the guidelines within 1 year after receipt
2 of the submission for approval.

3 (b) WITHDRAWAL OF APPROVAL.—If at any time the
4 Commission determines that the guidelines previously ap-
5 proved no longer meet the requirements of this Act or a
6 regulation promulgated under this Act or that compliance
7 with the approved guidelines is insufficiently enforced by
8 the independent organization administering the guidelines,
9 the Commission shall notify the covered entities or group
10 of such entities and the independent organization of the
11 determination of the Commission to withdraw approval of
12 such guidelines and the basis for doing so. Within 180 days
13 after receipt of such notice, the covered entity or group
14 of such entities and the independent organization may
15 cure any alleged deficiency with the guidelines or the en-
16 forcement of such guidelines and submit each proposed
17 cure to the Commission. If the Commission determines
18 that such cures eliminate the alleged deficiency in the
19 guidelines, then the Commission may not withdraw ap-
20 proval of such guidelines on the basis of such determina-
21 tion.

22 (c) DEEMED COMPLIANCE.—A covered entity that is
23 eligible to participate under subsection (a)(1) and partici-
24 pates in guidelines approved under this section shall be
25 deemed in compliance with the relevant provisions of this

1 Act if such covered entity is in compliance with such
2 guidelines.

3 **SEC. 304. DIGITAL CONTENT FORGERIES.**

4 (a) REPORTS.—Not later than 1 year after the date
5 of enactment of this Act, and annually thereafter, the Sec-
6 retary of Commerce or the Secretary’s designee shall pub-
7 lish a report regarding digital content forgeries.

8 (b) REQUIREMENTS.—Each report under subsection
9 (a) shall include the following:

10 (1) A definition of digital content forgeries
11 along with accompanying explanatory materials.

12 (2) A description of the common sources of dig-
13 ital content forgeries in the United States and com-
14 mercial sources of digital content forgery tech-
15 nologies.

16 (3) An assessment of the uses, applications, and
17 harms of digital content forgeries.

18 (4) An analysis of the methods and standards
19 available to identify digital content forgeries as well
20 as a description of the commercial technological
21 counter-measures that are, or could be, used to ad-
22 dress concerns with digital content forgeries, which
23 may include the provision of warnings to viewers of
24 suspect content.

1 (5) A description of the types of digital content
2 forgeries, including those used to commit fraud,
3 cause harm, or violate any provision of law.

4 (6) Any other information determined appro-
5 priate by the Secretary of Commerce or the Sec-
6 retary's designee.

7 **TITLE IV—ENFORCEMENT, AP-**
8 **PLICABILITY, AND MISCELLA-**
9 **NEOUS**

10 **SEC. 401. ENFORCEMENT BY THE FEDERAL TRADE COM-**
11 **MISSION.**

12 (a) BUREAU OF PRIVACY.—

13 (1) IN GENERAL.—The Commission shall estab-
14 lish within the Commission a new bureau to be
15 known as the “Bureau of Privacy”, which shall be
16 of similar structure, size, organization, and authority
17 as the existing bureaus within the Commission re-
18 lated to consumer protection and competition.

19 (2) MISSION.—The mission of the Bureau es-
20 tablished under paragraph (1) shall be to assist the
21 Commission in carrying out the duties of the Com-
22 mission under this Act and related duties under
23 other provisions of law.

24 (3) TIMELINE.—The Bureau required to be es-
25 tablished under paragraph (1) shall be established,

1 staffed, and fully operational not later than 1 year
2 after the date of enactment of this Act.

3 (b) OFFICE OF BUSINESS MENTORSHIP.—The Direc-
4 tor of the Bureau established under subsection (a)(1) shall
5 establish within the Bureau an office to be known as the
6 “Office of Business Mentorship” to provide guidance and
7 education to covered entities and service providers regard-
8 ing compliance with this Act. Covered entities or service
9 providers may request advice from the Commission or the
10 Office with respect to a course of action that the covered
11 entity or service provider proposes to pursue and that may
12 relate to the requirements of this Act.

13 (c) ENFORCEMENT BY THE FEDERAL TRADE COM-
14 MISSION.—

15 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
16 TICES.—A violation of this Act or a regulation pro-
17 mulgated under this Act shall be treated as a viola-
18 tion of a rule defining an unfair or deceptive act or
19 practice prescribed under section 18(a)(1)(B) of the
20 Federal Trade Commission Act (15 U.S.C.
21 57a(a)(1)(B)).

22 (2) POWERS OF THE COMMISSION.—

23 (A) IN GENERAL.—Except as provided in
24 paragraphs (3), (4), and (5), the Commission
25 shall enforce this Act and the regulations pro-

1 mulgated under this Act in the same manner,
2 by the same means, and with the same jurisdic-
3 tion, powers, and duties as though all applicable
4 terms and provisions of the Federal Trade
5 Commission Act (15 U.S.C. 41 et seq.) were in-
6 corporated into and made a part of this Act.

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

13 (3) LIMITING CERTAIN ACTIONS UNRELATED
14 TO THIS ACT.—If the Commission brings a civil ac-
15 tion alleging that an act or practice violates this Act
16 or a regulation promulgated under this Act, the
17 Commission may not seek a cease and desist order
18 against the same defendant under section 5(b) of the
19 Federal Trade Commission Act (15 U.S.C. 45(b)) to
20 stop that same act or practice on the grounds that
21 such act or practice constitutes an unfair or decep-
22 tive act or practice.

23 (4) COMMON CARRIERS AND NONPROFIT ORGA-
24 NIZATIONS.—Notwithstanding any jurisdictional lim-
25 itation of the Commission with respect to consumer

1 protection or privacy, the Commission shall enforce
2 this Act and the regulations promulgated under this
3 Act, in the same manner provided in paragraphs (1),
4 (2), (3), and (5), with respect to common carriers
5 subject to the Communications Act of 1934 (47
6 U.S.C. 151 et seq.) and all Acts amendatory thereof
7 and supplementary thereto and organizations not or-
8 ganized to carry on business for their own profit or
9 that of their members.

10 (5) PRIVACY AND SECURITY VICTIMS RELIEF
11 FUND.—

12 (A) ESTABLISHMENT.—There is estab-
13 lished in the Treasury of the United States a
14 separate fund to be known as the “Privacy and
15 Security Victims Relief Fund” in this para-
16 graph referred to as the “Victims Relief
17 Fund”).

18 (B) DEPOSITS.—Notwithstanding section
19 3302 of title 31, United States Code, in any ju-
20 dicial or administrative action to enforce this
21 Act or a regulation promulgated under this Act,
22 the amount of any civil penalty obtained against
23 a covered entity or service provider, or any
24 other monetary relief ordered to be paid by a
25 covered entity or service provider to provide re-

1 dress, payment, compensation, or other relief to
2 individuals that cannot be located or the pay-
3 ment of which would otherwise not be prac-
4 ticable, shall be deposited into the Victims Re-
5 lief Fund.

6 (C) USE OF FUNDS.—

7 (i) USE BY COMMISSION.—Amounts in
8 the Victims Relief Fund shall be available
9 to the Commission, without fiscal year lim-
10 itation, to provide redress, payment, com-
11 pensation, or other monetary relief to indi-
12 viduals affected by an act or practice for
13 which relief has been obtained under this
14 Act.

15 (ii) OTHER PERMISSIBLE USES.—To
16 the extent that the individuals described in
17 clause (i) cannot be located or such re-
18 dress, payments, compensation, or other
19 monetary relief are otherwise not prac-
20 ticable, the Commission may use such
21 funds for the purpose of—

22 (I) funding the activities of the
23 Office of Business Mentorship estab-
24 lished under subsection (b); or

1 (II) engaging in technological re-
2 search that the Commission considers
3 necessary to enforce or administer
4 this Act.

5 **SEC. 402. ENFORCEMENT BY STATES.**

6 (a) CIVIL ACTION.—In any case in which the attor-
7 ney general or State Privacy Authority of a State has rea-
8 son to believe that an interest of the residents of that
9 State has been, may be, or is adversely affected by a viola-
10 tion of this Act or a regulation promulgated under this
11 Act by a covered entity or service provider, the attorney
12 general or State Privacy Authority may bring a civil action
13 in the name of the State, or as *parens patriae* on behalf
14 of the residents of the State. Any such action shall be
15 brought exclusively in an appropriate Federal district
16 court of the United States to—

17 (1) enjoin such act or practice;

18 (2) enforce compliance with this Act or such
19 regulation;

20 (3) obtain damages, civil penalties, restitution,
21 or other compensation on behalf of the residents of
22 such State; or

23 (4) obtain reasonable attorneys' fees and other
24 litigation costs reasonably incurred.

25 (b) RIGHTS OF THE COMMISSION.—

1 (1) IN GENERAL.—Except as provided in para-
2 graph (2), the attorney general or State Privacy Au-
3 thority of a State shall notify the Commission in
4 writing prior to initiating a civil action under sub-
5 section (a). Such notification shall include a copy of
6 the complaint to be filed to initiate such action.
7 Upon receiving such notification, the Commission
8 may intervene in such action as a matter of right
9 pursuant to the Federal Rules of Civil Procedure.

10 (2) FEASIBILITY.—If the notification required
11 by paragraph (1) is not feasible, the attorney gen-
12 eral or State Privacy Authority shall notify the Com-
13 mission immediately after initiating the civil action.

14 (c) ACTIONS BY THE COMMISSION.—In any case in
15 which a civil action is instituted by or on behalf of the
16 Commission for violation of this Act or a regulation pro-
17 mulgated under this Act, no attorney general or State Pri-
18 vacy Authority of a State may, during the pendency of
19 such action, institute a civil action against any defendant
20 named in the complaint in the action instituted by or on
21 behalf of the Commission for a violation of this Act or
22 a regulation promulgated under this Act that is alleged
23 in such complaint, if such complaint alleges such violation
24 affected the residents of such State or individuals nation-
25 wide. If the Commission brings a civil action against a

1 covered entity or service provider for a violation of this
2 Act or a regulation promulgated under this Act that af-
3 fects the interests of the residents of a State, the attorney
4 general or State Privacy Authority of such State may in-
5 tervene in such action as a matter of right pursuant to
6 the Federal Rules of Civil Procedure.

7 (d) RULE OF CONSTRUCTION.—Nothing in this sec-
8 tion may be construed to prevent the attorney general or
9 State Privacy Authority of a State from exercising the
10 powers conferred on the attorney general or State Privacy
11 Authority to conduct investigations, to administer oaths
12 or affirmations, or to compel the attendance of witnesses
13 or the production of documentary or other evidence.

14 (e) PRESERVATION OF STATE POWERS.—Except as
15 provided in subsection (c), nothing in this section may be
16 construed as altering, limiting, or affecting the authority
17 of the attorney general or State Privacy Authority of a
18 State to—

19 (1) bring an action or other regulatory pro-
20 ceeding arising solely under the law in effect in the
21 State that is preempted by this Act or under another
22 applicable Federal law; or

23 (2) exercise the powers conferred on the attor-
24 ney general or State Privacy Authority by the laws
25 of the State, including the ability to conduct inves-

1 tigations, administer oaths or affirmations, or com-
2 pel the attendance of witnesses or the production of
3 documentary or other evidence.

4 **SEC. 403. ENFORCEMENT BY PERSONS.**

5 (a) ENFORCEMENT BY PERSONS.—

6 (1) IN GENERAL.—Beginning on the date that
7 is 2 years after the date on which this Act takes ef-
8 fect, any person or class of persons for a violation
9 of this Act or a regulation promulgated under this
10 Act by a covered entity or service provider may
11 bring a civil action against such entity in any Fed-
12 eral court of competent jurisdiction.

13 (2) RELIEF.—In a civil action brought under
14 paragraph (1) in which a plaintiff prevails, the court
15 may award the plaintiff—

16 (A) an amount equal to the sum of any
17 compensatory damages;

18 (B) injunctive relief;

19 (C) declaratory relief; and

20 (D) reasonable attorney's fees and litiga-
21 tion costs.

22 (3) RIGHTS OF THE COMMISSION AND STATE
23 ATTORNEYS GENERAL.—

24 (A) IN GENERAL.—Prior to a person
25 bringing a civil action under paragraph (1),

1 such person shall notify the Commission and
2 the attorney general of the State where such
3 person resides in writing that such person in-
4 tends to bring a civil action under such para-
5 graph. Upon receiving such notice, the Commis-
6 sion and State attorney general shall each or
7 jointly make a determination and respond to
8 such person not later than 60 days after receiv-
9 ing such notice, as to whether they will inter-
10 vene in such action pursuant to the Federal
11 Rules of Civil Procedure. If a state attorney
12 general does intervene, they shall only be heard
13 with respect to the interests of the residents of
14 their State

15 (B) RETAINED AUTHORITY.—Subpara-
16 graph (A) may not be construed to limit the au-
17 thority of the Commission or any applicable
18 State attorney general or State Privacy Author-
19 ity to later commence a proceeding or civil ac-
20 tion or intervene by motion if the Commission
21 or State attorney general or State Privacy Au-
22 thority does not commence a proceeding or civil
23 action within the 60-day period.

24 (C) BAD FAITH.—Any written communica-
25 tion from counsel for an aggrieved party to a

1 covered entity or service provider requesting a
2 monetary payment from that covered entity or
3 service provider regarding a specific claim de-
4 scribed in a letter sent pursuant to subsection
5 (d), not including filings in court proceedings,
6 arbitrations, mediations, judgment collection
7 processes, or other communications related to
8 previously initiated litigation or arbitrations,
9 shall be considered to have been sent in bad
10 faith and shall be unlawful as defined in this
11 Act, if the written communication was sent
12 prior to the date that is 60 days after either a
13 State attorney general or the Commission has
14 received the notice required under subpara-
15 graph (A).

16 (4) FTC STUDY.—Beginning on the date that
17 is 5 years after the date of enactment of this Act
18 and every 5 years thereafter, the Commission’s Bu-
19 reau of Economics and Bureau of Privacy shall as-
20 sist the Commission in conducting a study to deter-
21 mine the economic impacts in the United States of
22 demand letters sent pursuant to this section and the
23 scope of the rights of a person under this section to
24 bring forth civil actions against covered entities and

1 service providers. Such study shall include the fol-
2 lowing:

3 (A) The impact on insurance rates in the
4 United States.

5 (B) The impact on the ability of covered
6 entities to offer new products or services.

7 (C) The impact on the creation and growth
8 of new startup companies, including new tech-
9 nology companies.

10 (D) Any emerging risks, benefits, and
11 long-term trends in relevant marketplaces, sup-
12 ply chains, and labor availability.

13 (E) The impact on reducing, preventing, or
14 remediating harms to individuals, including
15 from fraud, identity theft, spam, discrimination,
16 defective products, and violations of rights.

17 (F) The impact on the volume and severity
18 of data security incidents, and the ability to re-
19 spond to data security incidents.

20 (G) Other intangible direct and indirect
21 costs and benefits to individuals.

22 (5) REPORT TO CONGRESS.—Not later than 5
23 years after the first day on which persons and class-
24 es of persons are able to bring civil actions under
25 this subsection, and annually thereafter, the Com-

1 mission shall submit to the Committee on Energy
2 and Commerce of the House of Representatives and
3 the Committee on Commerce, Science, and Trans-
4 portation of the Senate a report that contains the
5 results of the study conducted under paragraph (4).

6 (b) ARBITRATION AGREEMENTS AND PRE-DISPUTE
7 JOINT ACTION WAIVERS.—

8 (1) PRE-DISPUTE ARBITRATION AGREE-
9 MENTS.—

10 (A) Notwithstanding any other provision of
11 law, no pre-dispute arbitration agreement with
12 respect to an individual under the age of 18 is
13 enforceable with regard to a dispute arising
14 under this Act.

15 (B) Notwithstanding any other provision of
16 law, no pre-dispute arbitration agreement is en-
17 forceable with regard to a dispute arising under
18 this Act concerning a claim related to gender or
19 partner-based violence or physical harm.

20 (2) PRE-DISPUTE JOINT-ACTION WAIVERS.—
21 Notwithstanding any other provision of law, no pre-
22 dispute joint-action waiver with respect to an indi-
23 vidual under the age of 18 is enforceable with regard
24 to a dispute arising under this Act.

1 (3) DEFINITIONS.—For purposes of this sub-
2 section:

3 (A) PRE-DISPUTE ARBITRATION AGREE-
4 MENT.—The term “pre-dispute arbitration
5 agreement” means any agreement to arbitrate a
6 dispute that has not arisen at the time of the
7 making of the agreement.

8 (B) PRE-DISPUTE JOINT-ACTION WAIV-
9 ER.—The term “pre-dispute joint-action waiv-
10 er” means an agreement, whether or not part
11 of a pre-dispute arbitration agreement, that
12 would prohibit or waive the right of 1 of the
13 parties to the agreement to participate in a
14 joint, class, or collective action in a judicial, ar-
15 bitral, administrative, or other related forum,
16 concerning a dispute that has not yet arisen at
17 the time of the making of the agreement.

18 (c) RIGHT TO CURE.—

19 (1) NOTICE.—Subject to paragraph (3), with
20 respect to a claim under this section for—

21 (A) injunctive relief; or

22 (B) an action against a covered entity or
23 service provider that meets the requirements of
24 section 209 of this Act, such claim may be
25 brought by a person or class of persons if—

1 prior to asserting such claim—the person or
2 class or persons provides to the covered entity
3 or service provider 45 days’ written notice iden-
4 tifying the specific provisions of this Act the
5 person or class of persons alleges have been or
6 are being violated.

7 (2) EFFECT OF CURE.—Subject to paragraph
8 (3), in the event a cure is possible, if within the 45
9 days the covered entity or service provider dem-
10 onstrates to the court that it has cured the noticed
11 violation or violations and provides the person or
12 class of persons an express written statement that
13 the violation or violations has been cured and that
14 no further violations shall occur, a claim for injunc-
15 tive relief shall not be permitted and may be reason-
16 ably dismissed.

17 (3) RULE OF CONSTRUCTION.—The notice de-
18 scribed in paragraph (1) and the reasonable dis-
19 missal in paragraph (2) shall not apply more than
20 once to any alleged underlying violation by the same
21 covered entity.

22 (d) DEMAND LETTER.—If a person or a identified
23 members of a class of persons represented by counsel in
24 regard to an alleged violation or violations of the Act and
25 has correspondence sent to a covered entity or service pro-

1 vider by counsel alleging a violation or violations of the
2 provisions of this Act and requests a monetary payment,
3 such correspondence shall include the following language:
4 “Please visit the website of the Federal Trade Commission
5 for a general description of your rights under the Amer-
6 ican Data Privacy and Protection Act” followed by a
7 hyperlink to the webpage of the Commission required
8 under section 201. If such correspondence does not include
9 such language and hyperlink, a civil action brought under
10 this section by such person or identified members of the
11 class of persons represented by counsel may be dismissed
12 without prejudice and shall not be reinstated until such
13 person or persons has complied with this subsection.

14 (e) APPLICABILITY.—

15 (1) IN GENERAL.—This section shall only apply
16 to a claim alleging a violation of section 102, 104,
17 202, 203, 204, 205(a), 205(b), 206(b)(3)(C),
18 207(a), 208(a), or 302, or a regulation promulgated
19 under any such section.

20 (2) EXCEPTION.—This section shall not apply
21 to any claim against a covered entity that has less
22 than \$25,000,000 per year in revenue, collects, proc-
23 esses, or transfers the covered data of fewer than
24 50,000 individuals, and derives less than 50 percent
25 of its revenue from transferring covered data.

1 **SEC. 404. RELATIONSHIP TO FEDERAL AND STATE LAWS.**

2 (a) FEDERAL LAW PRESERVATION.—

3 (1) IN GENERAL.—Nothing in this Act or a reg-
4 ulation promulgated under this Act may be con-
5 strued to limit—

6 (A) the authority of the Commission, or
7 any other Executive agency, under any other
8 provision of law;

9 (B) any requirement for a common carrier
10 subject to section 64.2011 of title 47, Code of
11 Federal Regulations (or any successor regula-
12 tion) regarding information security breaches;
13 or

14 (C) any other provision of Federal law, ex-
15 cept as otherwise provided in this Act.

16 (2) ANTITRUST SAVINGS CLAUSE.—

17 (A) FULL APPLICATION OF THE ANTI-
18 TRUST LAW.—Nothing in this Act may be con-
19 strued to modify, impair or supersede the oper-
20 ation of the antitrust law or any other provision
21 of law.

22 (B) NO IMMUNITY FROM THE ANTITRUST
23 LAW.—Nothing in the regulatory regime adopt-
24 ed by this Act shall be construed as operating
25 to limit any law deterring anticompetitive con-
26 duct or diminishing the need for full application

1 of the antitrust law. Nothing in this Act explic-
2 itly or implicitly precludes the application of the
3 antitrust law.

4 (C) DEFINITION OF ANTITRUST LAW.—For
5 purposes of this section, the term antitrust law
6 has the same meaning as in subsection (a) of
7 the first section of the Clayton Act (15 U.S.C.
8 12), except that such term includes section 5 of
9 the Federal Trade Commission Act (15 U.S.C.
10 45) to the extent that such section 5 applies to
11 unfair methods of competition.

12 (3) APPLICABILITY OF OTHER PRIVACY RE-
13 QUIREMENTS.—A covered entity that is required to
14 comply with title V of the Gramm-Leach-Bliley Act
15 (15 U.S.C. 6801 et seq.), the Health Information
16 Technology for Economic and Clinical Health Act
17 (42 U.S.C. 17931 et seq.), part C of title XI of the
18 Social Security Act (42 U.S.C. 1320d et seq.), the
19 Fair Credit Reporting Act (15 U.S.C. 1681 et seq.),
20 the Family Educational Rights and Privacy Act (20
21 U.S.C. 1232g; part 99 of title 34, Code of Federal
22 Regulations) to the extent such covered entity is a
23 school as defined in 20 U.S.C. 1232g(a)(3) or 34
24 C.F.R. 99.1(a), section 444 of the General Edu-
25 cation Provisions Act (commonly known as the

1 “Family Educational Rights and Privacy Act of
2 1974”) (20 U.S.C. 1232g) and part 99 of title 34,
3 Code of Federal Regulations (or any successor regu-
4 lation), the Confidentiality of Alcohol and Drug
5 Abuse Patient Records at 42 U.S.C. 290dd-2 and its
6 implementing regulations at 42 CFR part 2, the Ge-
7 netic Information Non-discrimination Act (GINA),
8 or the regulations promulgated pursuant to section
9 264(c) of the Health Insurance Portability and Ac-
10 countability Act of 1996 (42 U.S.C. 1320d–2 note),
11 and is in compliance with the data privacy require-
12 ments of such regulations, part, title, or Act (as ap-
13 plicable), shall be deemed to be in compliance with
14 the related requirements of this Act, except for sec-
15 tion 208, solely and exclusively with respect to data
16 subject to the requirements of such regulations,
17 part, title, or Act. Not later than 1 year after the
18 date of enactment of this Act, the Commission shall
19 issue guidance describing the implementation of this
20 paragraph.

21 (4) APPLICABILITY OF OTHER DATA SECURITY
22 REQUIREMENTS.—A covered entity that is required
23 to comply with title V of the Gramm-Leach-Bliley
24 Act (15 U.S.C. 6801 et seq.), the Health Informa-
25 tion Technology for Economic and Clinical Health

1 Act (42 U.S.C. 17931 et seq.), part C of title XI of
2 the Social Security Act (42 U.S.C. 1320d et seq.),
3 or the regulations promulgated pursuant to section
4 264(c) of the Health Insurance Portability and Ac-
5 countability Act of 1996 (42 U.S.C. 1320d–2 note),
6 and is in compliance with the information security
7 requirements of such regulations, part, title, or Act
8 (as applicable), shall be deemed to be in compliance
9 with the requirements of section 208, solely and ex-
10 clusively with respect to data subject to the require-
11 ments of such regulations, part, title, or Act. Not
12 later than 1 year after the date of enactment of this
13 Act, the Commission shall issue guidance describing
14 the implementation of this paragraph.

15 (b) PREEMPTION OF STATE LAWS.—

16 (1) IN GENERAL.—No State or political subdivi-
17 sion of a State may adopt, maintain, enforce, pre-
18 scribe, or continue in effect any law, regulation, rule,
19 standard, requirement, or other provision having the
20 force and effect of law of any State, or political sub-
21 division of a State, covered by the provisions of this
22 Act, or a rule, regulation, or requirement promul-
23 gated under this Act.

24 (2) STATE LAW PRESERVATION.—Paragraph
25 (1) may not be construed to preempt, displace, or

1 supplant the following State laws, rules, regulations,
2 or requirements:

3 (A) Consumer protection laws of general
4 applicability, such as laws regulating deceptive,
5 unfair, or unconscionable practices, except that
6 the fact of a violation of this Act or a regula-
7 tion promulgated under this Act may not be
8 pleaded as an element of any violation of such
9 a law.

10 (B) Civil rights laws.

11 (C) Provisions of laws, in so far as, that
12 govern the privacy rights or other protections of
13 employees, employee information, students, or
14 student information.

15 (D) Laws that address notification require-
16 ments in the event of a data breach.

17 (E) Contract or tort law.

18 (F) Criminal laws.

19 (G) Civil laws governing fraud, theft (in-
20 cluding identity theft), unauthorized access to
21 information or electronic devices, unauthorized
22 use of information, malicious behavior, or simi-
23 lar provisions of law.

24 (H) Civil laws regarding cyberstalking,
25 cyberbullying, nonconsensual pornography, sex-

1 ual harassment, child abuse material, child por-
2 nography, child abduction or attempted child
3 abduction, coercion or enticement of a child for
4 sexual activity, or child sex trafficking.

5 (I) Public safety or sector specific laws un-
6 related to privacy or security.

7 (J) Provisions of law, insofar as such pro-
8 visions address public records, criminal justice
9 information systems, arrest records, mug shots,
10 conviction records, or non-conviction records.

11 (K) Provisions of law, insofar as such pro-
12 visions address banking records, financial
13 records, tax records, Social Security numbers,
14 credit cards, consumer and credit reporting and
15 investigations, credit repair, credit clinics, or
16 check-cashing services.

17 (L) Provisions of law, insofar as such pro-
18 visions address facial recognition or facial rec-
19 ognition technologies, electronic surveillance,
20 wiretapping, or telephone monitoring.

21 (M) The Biometric Information Privacy
22 Act (740 ICLS 14 et seq.) and the Genetic In-
23 formation Privacy Act (410 ILCS 513 et seq.).

24 (N) Provisions of laws, in so far as, such
25 provisions to address unsolicited email or text

1 messages, telephone solicitation, or caller identi-
2 fication.

3 (O) Provisions of laws, in so far as, such
4 provisions address health information, medical
5 information, medical records, HIV status, or
6 HIV testing.

7 (P) Provisions of laws, in so far as, such
8 provisions pertain to public health activities, re-
9 porting, data, or services.

10 (Q) Provisions of law, insofar as such pro-
11 visions address the confidentiality of library
12 records.

13 (R) Section 1798.150 of the California
14 Civil Code (as amended on November 3, 2020
15 by initiative Proposition 24, Section 16).

16 (S) Laws pertaining to the use of
17 encryption as a means of providing data secu-
18 rity.

19 (3) CPPA ENFORCEMENT.—Notwithstanding
20 any other provisions of law, the California Privacy
21 Protection Agency established under 1798.199.10(a)
22 of the California Privacy Rights Act may enforce
23 this Act, in the same manner, it would otherwise en-
24 force the California Consumer Privacy Act, Section
25 1798.1050 et. seq.

1 (4) NONAPPLICATION OF FCC PRIVACY LAWS
2 AND REGULATIONS TO CERTAIN COVERED ENTI-
3 TIES.—Notwithstanding any other provision of law,
4 sections 222, 338(i), and 631 of the Communica-
5 tions Act of 1934 (47 U.S.C. 222; 338(i); 551), and
6 any regulations and orders promulgated by the Fed-
7 eral Communications Commission under any such
8 section, do not apply to any covered entity with re-
9 spect to the collection, processing, transfer, or secu-
10 rity of covered data or its equivalent, and the related
11 privacy and data security activities of a covered enti-
12 ty that would otherwise be regulated under such sec-
13 tions shall be governed exclusively by the provisions
14 of this Act, except for—

15 (A) any emergency services, as defined in
16 section 7 of the Wireless Communications and
17 Public Safety Act of 1999 (47 U.S.C. 615b);

18 (B) subsections (b) and (g) of section 222
19 of the Communications Act of 1934 (47 U.S.C.
20 222); and

21 (C) any obligation of an international trea-
22 ty related to the exchange of traffic imple-
23 mented and enforced by the Federal Commu-
24 nications Commission.

1 (c) PRESERVATION OF COMMON LAW OR STATUTORY
2 CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this
3 Act, nor any amendment, standard, rule, requirement, as-
4 sessment, or regulation promulgated under this Act, may
5 be construed to preempt, displace, or supplant any Federal
6 or State common law rights or remedies, or any statute
7 creating a remedy for civil relief, including any cause of
8 action for personal injury, wrongful death, property dam-
9 age, or other financial, physical, reputational, or psycho-
10 logical injury based in negligence, strict liability, products
11 liability, failure to warn, an objectively offensive intrusion
12 into the private affairs or concerns of the individual, or
13 any other legal theory of liability under any Federal or
14 State common law, or any State statutory law.

15 **SEC. 405. SEVERABILITY.**

16 If any provision of this Act, or the application thereof
17 to any person or circumstance, is held invalid, the remain-
18 der of this Act, and the application of such provision to
19 other persons not similarly situated or to other cir-
20 cumstances, shall not be affected by the invalidation.

21 **SEC. 406. COPPA.**

22 (a) IN GENERAL.—Nothing in this Act may be con-
23 strued to relieve or change any obligation that a covered
24 entity or other person may have under the Children’s On-

1 line Privacy Protection Act of 1998 (15 U.S.C. 6501 et
2 seq.).

3 (b) UPDATED REGULATIONS.—Not later than 180
4 days after the date of enactment of this Act, the Commis-
5 sion shall amend its rules issued pursuant to the regula-
6 tions promulgated by the Commission under the Chil-
7 dren’s Online Privacy Protection Act of 1998 (15 U.S.C.
8 6501 et seq.) to make reference to the additional require-
9 ments placed on covered entities under this Act, in addi-
10 tion to the requirements under the Children’s Online Pri-
11 vacy Protection Act of 1998 that may already apply to
12 certain covered entities.

13 **SEC. 407. AUTHORIZATION OF APPROPRIATIONS.**

14 There are authorized to be appropriated to the Com-
15 mission such sums as may be necessary to carry out this
16 Act.

17 **SEC. 408. EFFECTIVE DATE.**

18 This Act shall take effect on the date that is 180 days
19 after the date of enactment of this Act.

