

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.

2 (a) **SHORT TITLE.**—This Act may be cited as the
3 “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. Service providers and third parties.
Sec. 303. Technical compliance programs.
Sec. 304. Commission approved compliance guidelines.

Sec. 305. Digital content forgeries.

TITLE IV—ENFORCEMENT, APPLICABILITY, AND MISCELLANEOUS

Sec. 401. Enforcement by the Federal Trade Commission.

Sec. 402. Enforcement by State Attorneys General.

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, informed, and
8 unambiguous authorization for an act or prac-
9 tice, in response to a specific request from a
10 covered entity that meets the requirements of
11 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.

1 (ii) The request includes a description
2 of the act or practice for which the individ-
3 ual's consent is sought and—

4 (I) clearly states the specific cat-
5 egories of covered data that the cov-
6 ered entity shall collect, process, and
7 transfer for each act or practice;

8 (II) clearly distinguishes between
9 any act or practice which is necessary
10 to fulfill a request of the individual
11 and any act or practice which is for
12 another purpose; and

13 (III) includes a prominent head-
14 ing and is written in easy-to-under-
15 stand language that would enable a
16 reasonable individual to identify and
17 understand 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 shall be made in a
2 manner readily accessible to and usable by
3 individuals with disabilities.

4 (v) The request shall be made avail-
5 able to the public in each language in
6 which the covered entity provides a product
7 or service for which authorization is sought
8 or in which the covered entity carries out
9 any activity related to any product or serv-
10 ice for which the covered data of the indi-
11 vidual may be collected, processed, or
12 transferred.

13 (C) EXPRESS CONSENT REQUIRED.—A
14 covered entity shall not infer that an individual
15 has provided affirmative express consent to an
16 act or practice from the inaction of the indi-
17 vidual or the individual's continued use of a
18 service or product provided by the covered enti-
19 ty.

20 (D) PRETEXTUAL CONSENT PROHIB-
21 ITED.—A covered entity shall not obtain or at-
22 tempt to obtain the affirmative express consent
23 of an individual through—

1 (i) the use of any false, fictitious,
2 fraudulent, or materially misleading state-
3 ment or representation; or

4 (ii) the design, modification, or ma-
5 nipulation of any user interface with the
6 purpose or substantial effect of obscuring,
7 subverting, or impairing a reasonable indi-
8 vidual's autonomy, decision making, or
9 choice to provide such consent or any cov-
10 ered data.

11 (2) ALGORITHM.—The term “algorithm” means
12 a computational process that uses machine learning,
13 natural language processing, artificial intelligence
14 techniques, or other computational processing tech-
15 niques of similar or greater complexity that makes
16 a decision or facilitate human decision-making with
17 respect to covered data, including to determine the
18 provision of products or services or to rank, order,
19 promote, recommend, amplify, or similarly determine
20 the delivery or display of information to an indi-
21 vidual.

22 (3) BIOMETRIC INFORMATION.—

23 (A) IN GENERAL.—The term “biometric
24 information” means any covered data generated
25 from the technological processing of an individ-

1 ual’s unique biological, physical, or physiological
2 characteristics that is linked or reasonably
3 linkable to an individual including—

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

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

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

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

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

1 (6) COMMON BRANDING.—The term “common
2 branding” means a name, service mark, or trade-
3 mark that is shared by 2 or more entities.

4 (7) CONTROL.—The term “control” means,
5 with respect to an entity—

6 (A) ownership of, or the power to vote,
7 more than 50 percent of the outstanding shares
8 of any class of voting security of the entity;

9 (B) control over the election of a majority
10 of the directors of the entity (or of individuals
11 exercising similar functions); or

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

14 (8) COVERED DATA.—

15 (A) IN GENERAL.—The term “covered
16 data” means information that identifies or is
17 linked or reasonably linkable, alone or in com-
18 bination with other information, to an indi-
19 vidual or a device that identifies or is linked or
20 reasonably linkable to an individual, and may
21 include derived data and unique identifiers.

22 (B) EXCLUSIONS.—The term “covered
23 data” does not include—

24 (i) de-identified data;

25 (ii) employee data;

- 1 (iii) publicly available information; or
2 (iv) inferences made exclusively from
3 multiple independent sources of publicly
4 available information that do not reveal
5 sensitive covered data with respect to an
6 individual.

7 (C) EMPLOYEE DATA DEFINED.—For pur-
8 poses of subparagraph (B), the term “employee
9 data” means—

10 (i) information relating to a job appli-
11 cant collected by a covered entity acting as
12 a prospective employer of such job appli-
13 cant in the course of the application, or
14 hiring process, provided that such informa-
15 tion is collected, processed, or transferred
16 by the prospective employer solely for pur-
17 poses related to the employee’s status as a
18 current or former job applicant of such
19 employer;

20 (ii) the business contact information
21 of an employee, including the employee’s
22 name, position or title, business telephone
23 number, business address, or business
24 email address that is provided to an em-
25 ployer by an employee who is acting in a

1 professional capacity, provided that such
2 information is collected, processed, or
3 transferred solely for purposes related to
4 such employee's professional activities;

5 (iii) emergency contact information
6 collected by an employer that relates to an
7 employee of that employer, provided that
8 such information is collected, processed, or
9 transferred solely for the purpose of having
10 an emergency contact on file for the em-
11 ployee; or

12 (iv) information relating to an em-
13 ployee (or a spouse, dependent, other cov-
14 ered family member, or beneficiary of such
15 employee) that is necessary for the em-
16 ployer to collect, process, or transfer solely
17 for the purpose of administering benefits
18 to which such employee (or spouse, de-
19 pendent, other covered family member, or
20 beneficiary of such employee) is entitled on
21 the basis of the employee's position with
22 that employer.

23 (9) COVERED ENTITY.—The term “covered en-
24 tity”—

1 (A) means any entity or any person, other
2 than an individual acting in a non-commercial
3 context, that alone or jointly with others deter-
4 mines the purposes and means of collecting,
5 processing, or transferring covered data and—

6 (i) is subject to the Federal Trade
7 Commission Act (15 U.S.C. 41 et seq.);

8 (ii) is a common carrier subject to the
9 Communications Act of 1934 (47 U.S.C.
10 151 et seq) and all Acts amendatory there-
11 of and supplementary thereto title II of the
12 Communications Act of 1934 (47 U.S.C.
13 201–231) as currently enacted or subse-
14 quently amended; or

15 (iii) is an organization not organized
16 to carry on business for their own profit or
17 that of their members; and

18 (B) includes any entity or person that con-
19 trols, is controlled by, or is under common con-
20 trol with another covered entity.

21 (C) EXCLUSIONS.—The term “covered en-
22 tity” does not include—

23 (i) a governmental entity such as a
24 body, authority, board, bureau, commis-
25 sion, district, agency, or political subdivi-

1 sion of the Federal, State, or local govern-
2 ment;

3 (ii) a person or an entity that is col-
4 lecting, processing, or transferring covered
5 data on behalf of or a Federal, State, Trib-
6 al, territorial, or local government entity.

7 (10) DE-IDENTIFIED DATA.—The term “de-
8 identified data” means information that does not
9 identify and is not linked or reasonably linkable to
10 an individual or an individual’s device, regardless of
11 whether the information is aggregated, provided that
12 the covered entity—

13 (A) takes reasonable technical, administra-
14 tive, and physical measures to ensure that the
15 information cannot, at any point, be used to re-
16 identify any individual or device;

17 (B) publicly commits in a clear and con-
18 spicuous manner—

19 (i) to process and transfer the infor-
20 mation solely in a de-identified form with-
21 out any reasonable means for re-identifica-
22 tion; and

23 (ii) to not attempt to re-identify the
24 information with any individual or device;
25 and

1 (C) contractually obligates any person or
2 entity that receives the information from the
3 covered entity to comply with all of the provi-
4 sions of this paragraph.

5 (11) DERIVED DATA.—The term “derived data”
6 means covered data that is created by the derivation
7 of information, data, assumptions, correlations, in-
8 ferences, predictions, or conclusions from facts, evi-
9 dence, or another source of information or data
10 about an individual or an individual’s device.

11 (12) DEVICE.—The term “device” means any
12 electronic equipment capable of transmitting or re-
13 ceiving covered data that is designed for use by one
14 or more individuals.

15 (13) EMPLOYEE.—The term “employee” means
16 (regardless of whether such employee is paid, un-
17 paid, or employed on a temporary basis) an em-
18 ployee, director, officer, staff member, an individual
19 working as a contractor, trainee, volunteer, or intern
20 of an employer.

21 (14) EXECUTIVE AGENCY.—The “Executive
22 agency” has the meaning set forth in section 105 of
23 title 5, United States Code.

24 (15) GENETIC INFORMATION.—The term “ge-
25 netic information” means any covered data, regard-

1 less of its format, that concerns an individual’s ge-
2 netic characteristics, including—

3 (A) raw sequence data that results from
4 the sequencing of an individual’s complete ex-
5 tracted or a portion of the extracted
6 deoxyribonucleic acid (DNA); or

7 (B) genotypic and phenotypic information
8 that results from analyzing the raw sequence
9 data.

10 (16) INDIVIDUAL.—The term “individual”
11 means a natural person residing in the United
12 States.

13 (17) LARGE DATA HOLDER.—The term “large
14 data holder” means a covered entity or service pro-
15 vider that, in the most recent calendar year—

16 (A) had annual gross revenues of
17 \$250,000,000 or more; and

18 (B) collected, processed, or transferred—

19 (i) the covered data of more than
20 5,000,000 individuals or devices that iden-
21 tify or are linked or reasonably linkable to
22 1 or more individuals; and

23 (ii) the sensitive covered data of more
24 than 200,000 individuals or devices that

1 identify or are linked or reasonably
2 linkable to 1 or more individuals.

3 (C) EXCLUSIONS.—The term “large data
4 holder” does not include any instance where the
5 covered entity or service provider would qualify
6 as a large data holder solely on account of col-
7 lecting, or processing—

8 (i) personal email addresses;

9 (ii) personal telephone numbers; or

10 (iii) log-in information of an indi-
11 vidual or device to allow the individual or
12 device to log in to an account administered
13 by the covered entity or service provider.

14 (D) REVENUE.—For purposes of this de-
15 termining whether any covered entity or service
16 provider is a large data holder, the term “rev-
17 enue” as it relates to any covered entity or
18 service provider that is not organized to carry
19 on business for its own profit or that of its
20 members, means the gross receipts the covered
21 entity or service provider received in whatever
22 form from all sources without subtracting any
23 costs or expenses, and includes contributions,
24 gifts, grants, dues or other assessments, income

1 from investments, or proceeds from the sale of
2 real or personal property.

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

9 (A) integrated into any product or service;

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

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

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

23 (20) PRECISE GEOLOCATION INFORMATION.—

24 (A) IN GENERAL.—The term “precise
25 geolocation information” means information

1 that reveals the past or present physical loca-
2 tion of an individual, or device that identifies or
3 is linked or reasonably linkable to 1 or more in-
4 dividuals, with sufficient precision to identify
5 street level location information or an individ-
6 ual’s location within a range of 1,000 feet or
7 less.

8 (B) EXCLUSION.—The term “precise
9 geolocation information” does not mean
10 geolocation information identifiable solely from
11 the visual content of an image.

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

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

24 (23) PUBLICLY AVAILABLE INFORMATION.—

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

6 (i) Federal, State, or local government
7 records provided that the covered entity
8 collects, processes and transfers such infor-
9 mation in accordance with any restrictions
10 or terms of use placed on the information
11 by the relevant government entity;

12 (ii) widely distributed media;

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

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

21 (v) a visual observation of an individ-
22 ual’s physical presence in a public place by
23 another person, not including data col-
24 lected by a device in the individual’s pos-
25 session.

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 for purposes of section
15 1460 of title 18, United States Code);

16 (II) inferences made exclusively
17 from multiple independent sources of
18 publicly available information that do
19 not reveal sensitive covered data with
20 respect to an individual;

21 (III) biometric information;

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

25 (V) genetic information; or

1 (VI) known nonconsensual inti-
2 mate images.

3 (24) SENSITIVE COVERED DATA.—

4 (A) IN GENERAL.—The term “sensitive
5 covered data” means the following forms of cov-
6 ered data:

7 (i) A government-issued identifier,
8 such as a social security number, passport
9 number, or driver’s license number, that is
10 not required by law to be displayed in pub-
11 lic.

12 (ii) Any information that describes or
13 reveals the past, present, or future physical
14 health, mental health, disability, diagnosis,
15 or healthcare condition or treatment of an
16 individual.

17 (iii) A financial account number, debit
18 card number, credit card number, or infor-
19 mation about income level or bank account
20 balances.

21 (iv) Biometric information.

22 (v) Genetic information.

23 (vi) Precise geolocation information.

24 (vii) An individual’s private commu-
25 nications such as voicemails, emails, texts,

1 direct messages, or mail, or information
2 identifying the parties to such communica-
3 tions, voice communications, and any infor-
4 mation that pertains to the transmission of
5 such communications, including telephone
6 numbers called, telephone numbers from
7 which calls were placed, the time calls were
8 made, call duration, and location informa-
9 tion of the parties to the call, unless the
10 covered entity is the sender or an intended
11 recipient of the communication. Commu-
12 nications are not private for purposes of
13 this paragraph if such communications are
14 made from or to a device provided by an
15 employer to an employee insofar as such
16 employer provides conspicuous notice that
17 it may access such communications.

18 (viii) Account or device log-in creden-
19 tials, or security or access codes for an ac-
20 count or device.

21 (ix) Information identifying the sexual
22 orientation or sexual behavior of an indi-
23 vidual in a manner inconsistent with the
24 individual's reasonable expectation regard-
25 ing disclosure of such information.

1 (x) Calendar information, address
2 book information, phone or text logs,
3 photos, audio recordings, or videos main-
4 tained for private use by an individual, re-
5 gardless of whether such information is
6 stored on the individual's device or in a
7 separate location on an individual's device,
8 regardless of whether such information is
9 backed up in a separate location.

10 (xi) A photograph, film, video record-
11 ing, or other similar medium that shows
12 the naked or undergarment-clad private
13 area of an individual.

14 (xii) Information that reveals the
15 video content or services requested or se-
16 lected by an individual from a provider of
17 broadcast television service, cable service,
18 satellite service or streaming media service.

19 (xiii) Information about an individual
20 when the covered entity knows that the in-
21 dividual is under the age of 17.

22 (xiv) Any other covered data collected,
23 processed, or transferred for the purpose
24 of identifying the above data types.

1 (B) RULEMAKING.—The Commission may
2 commence a rulemaking pursuant to section
3 553 of title 5, United States Code, to include
4 any additional category of covered data under
5 this definition that may require a similar level
6 of protection as the data listed in clauses (i)
7 through (xvi) of subparagraph (A) as a result
8 of any new method of collecting, processing, or
9 transferring covered data.

10 (25) SERVICE PROVIDER.—The term “service
11 provider” means a person or entity that collects,
12 processes or transfers covered data on behalf of, and
13 at the direction of, a covered entity and which re-
14 ceives covered data from or on behalf of a covered
15 entity pursuant to a written contract, provided that
16 the contract meets the requirements of section 302.

17 (26) SERVICE PROVIDER DATA.—The term
18 “service provider data” means covered data that is
19 collected or processed by or has been transferred to
20 a service provider by a covered entity for the pur-
21 pose of allowing the service provider to perform a
22 service or function on behalf of, and at the direction
23 of, such covered entity.

24 (27) STATE.—The term “State” means any of
25 the 50 States, the District of Columbia, the Com-

1 monwealth of Puerto Rico, the Virgin Islands,
2 Guam, American Samoa, the Northern Mariana Is-
3 lands, or the Trust Territory of the Pacific Islands.

4 (28) STATE PRIVACY AUTHORITY.—

5 (A) IN GENERAL.—The term “State Pri-
6 vacy Authority” means—

7 (i) the chief consumer protection offi-
8 cer of a State; or

9 (ii) a State consumer protection agen-
10 cy with expertise in data protection.

11 (29) SUBSTANTIAL PRIVACY RISK.—The term
12 “substantial privacy risk” means the collection,
13 processing, or transfer of covered data in a manner
14 that may result in any reasonably foreseeable mate-
15 rial physical injury, economic injury, highly offensive
16 intrusion into the reasonable privacy expectations of
17 an individual under the circumstances, or discrimi-
18 nation on the basis of race, color, religion, national
19 origin, sex, or disability.

20 (30) TARGETED ADVERTISING.—The term “tar-
21 geted advertising”—

22 (A) means displaying to an individual or
23 device identified by a unique identifier an online
24 advertisement or content that is selected based
25 on known or predicted preferences, characteris-

1 tics, or interests associated with the individual
2 or a device identified by a unique identifier; and

3 (B) does not include—

4 (i) advertising or marketing to an in-
5 dividual or an individual’s device in re-
6 sponse to the individual’s specific request
7 for information or feedback;

8 (iii) contextual advertising, which is
9 when an advertisement is displayed based
10 on the content or location in which the ad-
11 vertisement appears and does not vary
12 based on who is viewing the advertisement;
13 or

14 (iv) processing covered data solely for
15 measuring or reporting advertising or con-
16 tent, performance, reach, or frequency, in-
17 cluding independent measurement.

18 (31) THIRD PARTY.—The term “third party”—

19 (A) means any person or entity that—

20 (i) collects, processes, or transfers
21 third party data; and

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

24 (B) does not include a person or entity
25 that collects covered data from another entity if

1 the 2 entities are related by common ownership
2 or corporate control and share common brand-
3 ing, unless one of those is a large data holder
4 or those entities are each related to a large data
5 holder through common ownership or corporate
6 control.

7 (32) THIRD-PARTY COLLECTING ENTITY.—

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

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

16 (ii) does not include a covered entity
17 in so far as such entity processes employee
18 data collected by and received from a third
19 party concerning any individual who is an
20 employee of the third party for the sole
21 purpose of such third party providing ben-
22 efits to the employee.

23 (B) PRINCIPAL SOURCE OF REVENUE DE-
24 FINED.—For purposes of this paragraph, “prin-

1 cial source of revenue” means, for the prior
2 12-month period, either—

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

5 (ii) obtaining revenue from processing
6 or transferring the covered data of more
7 than 5,000,000 individuals that the cov-
8 ered entity did not collect directly from the
9 individuals to which the covered data per-
10 tains.

11 (C) NON-APPLICATION TO SERVICE PRO-
12 VIDERS.—An entity shall not be considered to
13 be a third-party collecting entity for purposes of
14 this Act if the entity is acting as a service pro-
15 vider (as defined in this section).

16 (33) THIRD PARTY DATA.—The term “third
17 party data” means covered data that has been trans-
18 ferred to a third party by a covered entity.

19 (34) TRANSFER.—The term “transfer” means
20 – to disclose, release, share, disseminate, make avail-
21 able, or license in writing, electronically, or by any
22 other means.

23 (35) UNIQUE IDENTIFIER.—The term “unique
24 identifier” means an identifier to the extent that
25 such identifier is reasonably linkable to an individual

1 or device that identifies or is linked or reasonably
2 linkable to 1 or more individuals, including a device
3 identifier, an Internet Protocol address, cookies, bea-
4 cons, pixel tags, mobile ad identifiers, or similar
5 technology, customer number, unique pseudonym, or
6 user alias, telephone numbers, or other forms of per-
7 sistent or probabilistic identifiers that are linked or
8 reasonably linkable to an individual or device.

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

18 **TITLE I—DUTY OF LOYALTY**

19 **SEC. 101. DATA MINIMIZATION.**

20 (a) IN GENERAL.—A covered entity shall not collect,
21 process, or transfer covered data unless the collection,
22 processing, or transfer is limited to what is reasonably
23 necessary and proportionate to—

1 (1) provide, or maintain a specific product or
2 service requested by the individual to whom the data
3 pertains;

4 (2) deliver a communication that is reasonably
5 anticipated by the individual recipient within the
6 context of the individual's interactions with the cov-
7 ered entity; or

8 (3) effect a purpose expressly permitted under
9 subsection (b).

10 (b) PERMISSIBLE PURPOSES.—A covered entity or
11 service provider may collect, process, or transfer covered
12 data for any of the following purposes provided that the
13 covered entity or service provider can demonstrate that
14 collection, processing, or transfer complies with all other
15 applicable laws not preempted in section 404 and provi-
16 sions of this Act and is limited to what is reasonably nec-
17 essary and proportionate to such purpose:

18 (1) To initiate or complete a transaction or ful-
19 fill an order or service specifically requested by an
20 individual, including any associated routine adminis-
21 trative activity such as billing, shipping, delivery,
22 and accounting, including the collection, processing
23 or transferring of the last four digits of a credit card
24 number.

1 (2) With respect to covered data previously col-
2 lected in accordance with this Act, notwithstanding
3 this exception, to process such data as necessary to
4 perform system maintenance or diagnostics, to main-
5 tain a product or service for which such data was
6 collected, to conduct internal research or analytics,
7 to improve a product or service for which such data
8 was collected and to perform inventory management
9 or reasonable network management, to protect
10 against spam, or to debug or repair errors that im-
11 pair the functionality of a service or product for
12 which such data was collected.

13 (3) To authenticate users of a product or serv-
14 ice.

15 (4) To prevent, detect, protect against, or re-
16 spond to a security incident, or fulfill a product or
17 service warranty. For purposes of this paragraph,
18 security is defined as network security as well as in-
19 trusion, medical alerts, fire alarms, and access con-
20 trol security.

21 (5) To prevent, detect, protect against or re-
22 spond to fraud, harassment, or illegal activity. For
23 the purposes of this paragraph, illegal activity means
24 a violation of a Federal, State, or local law punish-

1 able as a felony or misdemeanor that can directly
2 harm another person.

3 (6) To comply with a legal obligation imposed
4 by Federal, Tribal, Local, or State law, or to estab-
5 lish, exercise, or defend legal claims.

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

12 (8) To effectuate a product recall pursuant to
13 Federal or State law.

14 (9)(A) To conduct a public or peer-reviewed sci-
15 entific, historical, or statistical research project
16 that—

17 (i) is in the public interest;

18 (ii) adheres to all relevant laws governing
19 such research; and

20 (iii) adheres to the regulations for human
21 subject research established under part 46 of
22 title 45, Code of Federal Regulations (or a suc-
23 cessor regulations).

24 (B) The Commission should set forth within 18
25 months of the enactment of this Act guidelines to

1 help covered entities ensure the privacy of affected
2 users and the security of covered data, particularly
3 as data is being transferred to and stored by re-
4 searchers.

5 (10) To deliver a communication at the direc-
6 tion of an individual between the communicating in-
7 dividual and one or more individuals or entities.

8 (11) With respect to covered data previously
9 collected in accordance with this Act, notwith-
10 standing this exception, to process such data as nec-
11 essary to provide first party marketing or adver-
12 tising of products or services provided by the covered
13 entity.

14 (12) Otherwise complies with the requirements
15 of this Act, including section 204(c), to provide a
16 targeted advertisement.

17 (c) GUIDANCE.—The Commission shall issue guid-
18 ance regarding what is reasonably necessary
19 and proportionate to comply with this section. Such guid-
20 ance shall take into consideration—

21 (1) the size of, and the nature, scope, and com-
22 plexity of the activities engaged in by the covered en-
23 tity, including whether the covered entity is a large
24 data holder, nonprofit organization, covered entities

1 meeting the requirements of section 209, service pro-
2 vider, third party, or third-party collecting entity;

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

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

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

10 (d) DECEPTIVE MARKETING OF A PRODUCT OR
11 SERVICE.—A covered entity, service provider, or third
12 party is prohibited from engaging in deceptive advertising
13 or marketing with respect to a product or service provided
14 to an individual.

15 **SEC. 102. LOYALTY DUTIES.**

16 (a) RESTRICTED DATA PRACTICES.—Notwith-
17 standing section 101 and unless an exception applies, with
18 respect to covered data, a covered entity shall not—

19 (1) collect, process, or transfer a social security
20 number, except when necessary to facilitate exten-
21 sions of credit, authentication, the payment and col-
22 lection of taxes, the enforcement of a contract be-
23 tween parties, or the prevention, investigation, and
24 prosecution of fraud or illegal activity;

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 to effect a purpose enu-
6 merated in section 101(b)(1) through (10);

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

9 (A) the transfer is made pursuant to the
10 affirmative express consent of the individual;

11 (B) the transfer is necessary to comply
12 with a legal obligation imposed by Federal,
13 State, or local law, or to establish, exercise, or
14 defend legal claims; or

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

20 (D) the transfer of biometric information
21 is necessary to facilitate data security or au-
22 thentication;

23 (E) the transfer of a password is necessary
24 to use a designated password manager or is to
25 a covered entity for the exclusive purpose of

1 identifying passwords that are being re-used
2 across sites or accounts; or

3 (F) the transfer of genetic information is
4 necessary to perform a medical diagnosis or
5 medical treatment specifically requested by an
6 individual, or to conduct medical research in ac-
7 cordance with conditions of section 101(b)(9);
8 or

9 (4) collect, process, or transfer an individual's
10 aggregated internet search or browsing history, ex-
11 cept with the affirmative express consent of the indi-
12 vidual or pursuant to one of the permissible pur-
13 poses enumerated in section 101(b)(1) through (10).

14 **SEC. 103. PRIVACY BY DESIGN.**

15 (a) POLICIES, PRACTICES, AND PROCEDURES.—A
16 covered entity and a service provider shall establish, imple-
17 ment, and maintain reasonable policies, practices, and pro-
18 cedures regarding the collection, processing, and transfer
19 of covered data to—

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

23 (2) identify, assess, and mitigate privacy risks
24 related to individuals under the age of 17, if applica-
25 ble

1 (3) mitigate privacy risks, including substantial
2 privacy risks, related to the products and services of
3 the covered entity or the service provider, including
4 their design, development, and implementation; 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.

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

16 (1) the size of the covered entity or the service
17 provider and the nature, scope, and complexity of
18 the activities engaged in by the covered entity, in-
19 cluding whether the covered entity is a large data
20 holder, nonprofit organization, covered entities meet-
21 ing the requirements of section 209, third party, or
22 third-party collecting entity;

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

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

4 (4) the number of individuals and devices to
5 which the covered data collected, processed, or trans-
6 ferred by the covered entity or service provider re-
7 lates; and

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

11 (c) COMMISSION GUIDANCE.—Not later than 1 year
12 after the date of enactment of this Act, the Commission
13 shall issue guidance as to what constitutes reasonable poli-
14 cies, practices, and procedures as required by this section.
15 The Commission shall consider unique circumstances ap-
16 plicable to nonprofit organizations and covered entities
17 meeting the requirements of section 209.

18 **SEC. 104. LOYALTY TO INDIVIDUALS WITH RESPECT TO**
19 **PRICING.**

20 (a) CONDITIONAL SERVICE OR PRICING PROHIB-
21 ITED.—A covered entity shall not deny or condition or ef-
22 fectively condition the provision of a service or product to
23 an individual based on the individual's agreement to waive
24 (or refusal to waive) any requirements under this Act or
25 any regulations promulgated under this Act or terminate

1 a service or otherwise refuse to provide a service or prod-
2 uct to an individual as a consequence of the individual's
3 refusal to provide such a waiver.

4 (b) RULES OF CONSTRUCTION.—Nothing in sub-
5 section (a) shall be construed to—

6 (1) prohibit the relation of the price of a service
7 or the level of service provided to an individual to
8 the provision, by the individual, of financial informa-
9 tion that is necessarily collected and processed only
10 for the purpose of initiating, rendering, billing for,
11 or collecting payment for a service or product re-
12 quested by the individual;

13 (2) prohibit a covered entity from offering a
14 loyalty program that provides discounted or free
15 products or services, or other consideration, in ex-
16 change for an individual's continued business with
17 the covered entity, provided that such program oth-
18 erwise complies with the requirements of this Act
19 and any regulations promulgated under this Act;

20 (3) require a covered entity to provide a loyalty
21 program that would require the covered entity to col-
22 lect, process, or transfer covered data that it other-
23 wise would not;

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

4 (5) prohibit a covered entity from offering dif-
5 ferent types of pricing or functionalities with respect
6 to a product or service based on an individual's exer-
7 cise of a right in section 203(a)(3).

8 **TITLE II—CONSUMER DATA**
9 **RIGHTS**

10 **SEC. 201. CONSUMER AWARENESS.**

11 (a) IN GENERAL.—Not later than 90 days after the
12 date of enactment of this Act, the Commission shall pub-
13 lish, on the public website of the Commission, a webpage
14 that describes each provision, right, obligation, and re-
15 quirement of this Act, listed separately for individuals and
16 for covered entities and service providers, and the rem-
17 edies, exemptions, and protections associated with this Act
18 in plain and concise language and in an easy-to-under-
19 stand manner.

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

24 (c) ACCESSIBILITY.—The Commission shall publish
25 materials disclosed pursuant to subsection (a) in the ten

1 languages with the most users in the United States, ac-
2 cording to the most recent U.S. Census. The Commission
3 shall ensure the website is readily accessible to and usable
4 by individuals with disabilities.

5 **SEC. 202. TRANSPARENCY.**

6 (a) IN GENERAL.—Each covered entity and service
7 provider shall make publicly available, in a clear, con-
8 spicuous, not misleading, and readily accessible manner,
9 a privacy policy that provides a detailed and accurate rep-
10 resentation of the entity’s data collection, processing, and
11 transfer activities.

12 (b) CONTENT OF PRIVACY POLICY.—The privacy pol-
13 icy required under subsection (a) shall include, at a min-
14 imum, the following:

15 (1) The identity and the contact information
16 of—

17 (A) the covered entity or service provider
18 (including the covered entity’s or service pro-
19 vider’s points of contact, generic electronic mail
20 addresses, and phone numbers of the covered
21 entity, as applicable for privacy and data secu-
22 rity inquiries); and

23 (B) any other entity within the same cor-
24 porate structure as, and under common brand-
25 ing with, the covered entity or service provider

1 to which covered data is transferred by the cov-
2 ered entity.

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

5 (3) The processing purposes for each category
6 of covered data the covered entity or service provider
7 collects or processes.

8 (4) Whether the covered entity or service pro-
9 vider transfers covered data and, if so, each category
10 of service provider and third party to which the cov-
11 ered entity or service provider transfers covered
12 data, the name of each third-party collecting entity
13 to which the covered entity or service provider trans-
14 fers covered data, and the purposes for which such
15 data is transferred to such categories of service pro-
16 viders and third parties or third-party collecting en-
17 tities, except for transfers to governmental entities
18 pursuant to a court order or law that prohibits the
19 covered entity from disclosing such transfer.

20 (5) The length of time the covered entity or
21 service provider intends to retain each category of
22 covered data, including sensitive covered data, or, if
23 it is not possible to identify that time frame, the cri-
24 teria used to determine the length of time the cov-

1 ered entity intends to retain categories of covered
2 data.

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

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

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

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

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

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

18 (2) carries out activities related to such product
19 or service.

20 (d) ACCESSIBILITY.—The covered entity or service
21 provider shall also provide the disclosures under this sec-
22 tion in a manner that is readily accessible to and usable
23 by individuals with disabilities.

24 (e) MATERIAL CHANGES.—

1 (1) AFFIRMATIVE EXPRESS CONSENT.—If a
2 covered entity makes a material change to its pri-
3 vacy policy or practices, the covered entity shall no-
4 tify each individual affected by such material change
5 before implementing the material change with re-
6 spect to any previously collected covered data and,
7 except as provided in section 101(b), provide a rea-
8 sonable opportunity for each individual to withdraw
9 consent to any further materially different collection,
10 processing or transferring of covered data under the
11 changed policy.

12 (2) NOTIFICATION.—The covered entity shall
13 take all reasonable measures to provide direct notifi-
14 cation regarding material changes to the privacy pol-
15 icy to each affected individual, in each language that
16 the privacy policy is made available, and taking into
17 account available technology and the nature of the
18 relationship.

19 (3) CLARIFICATION.—Nothing in this section
20 shall be construed to affect the requirements for cov-
21 ered entities under section 102 or 204.

22 (4) LOG OF MATERIAL CHANGES.—each large
23 data holder shall retain copies of previous versions
24 of its privacy policy for at least 10 years and publish
25 them on its website. It shall make publicly available,

1 in a clear, conspicuous, and readily accessible man-
2 ner, a log describing the data and nature of each
3 material change over the past 10 years. The descrip-
4 tions shall be sufficient for a reasonable individual
5 to understand the material effect of each material
6 change.

7 (f) SHORT-FORM NOTICE TO CONSUMERS BY LARGE
8 DATA HOLDERS.—

9 (1) IN GENERAL.—In addition to the privacy
10 policy required under subsection (a), a large data
11 holder must provide a short-form notice of its cov-
12 ered data practices in a manner that is—

13 (A) concise, clear, and conspicuous;

14 (B) readily accessible, based on the way an
15 individual interacts with the large data holder
16 and its products or services and what is reason-
17 ably anticipated within the context of the rela-
18 tionship;

19 (C) inclusive of an overview of individual
20 rights and disclosures to reasonably draw atten-
21 tion to data practices that may reasonably be
22 unexpected or that involve sensitive covered
23 data; and

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

1 (2) RULEMAKING.—The Commission shall issue
2 a rule pursuant to section 553 of title 5, United
3 States Code, establishing the minimum data disclo-
4 sures necessary for the short-form notice which shall
5 not exceed the content requirements in subsection
6 (b) and shall include templates and/or models of
7 short-form notices.

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

9 (a) ACCESS TO, AND CORRECTION, DELETION, AND
10 PORTABILITY OF, COVERED DATA.—Subject to sub-
11 sections (b) and (c), a covered entity shall provide an indi-
12 vidual, after receiving a verified request from the indi-
13 vidual, with the right to—

14 (1) access—

15 (A) the covered data, except covered data
16 in back-up or archival systems, of the individual
17 in a human-readable format that a reasonable
18 individual can understand and download from
19 the Internet, that is collected, processed or
20 transferred by the covered entity or any service
21 provider of the covered entity within the 24
22 months preceding the request;

23 (B) the name of any third party and the
24 categories of any service providers to whom the
25 covered entity has transferred for consideration

1 the covered data of the individual, as well as
2 the categories of sources from which the cov-
3 ered data was collected; and

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

8 (2) correct any verifiably material inaccuracy or
9 materially incomplete information with respect to the
10 covered data of the individual that is processed by
11 the covered entity and instruct the covered entity to
12 notify any third party, or service provider to which
13 the covered entity transferred such covered data of
14 the corrected 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 notify any third party, or service pro-
18 vider to which the covered entity transferred such
19 covered data of the individual's deletion request; and

20 (4) to the extent technically feasible, export cov-
21 ered data to the individual or directly to another en-
22 tity, except for derived data, of the individual that
23 is processed by the covered entity without licensing
24 restrictions that limit such transfers, in—

1 (A) a human-readable format that a rea-
2 sonable individual can understand and
3 download from the Internet; and

4 (B) a portable, structured, interoperable,
5 and machine-readable format.

6 (b) INDIVIDUAL AUTONOMY.—A covered entity shall
7 not condition, effectively condition, attempt to condition,
8 or attempt to effectively condition the exercise of any indi-
9 vidual rights under this section through—

10 (1) through the use of any false, fictitious,
11 fraudulent, or materially misleading statement or
12 representation; or

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

18 (c) TIMING.—

19 (1) Subject to subsections (d) and (e)(1) each
20 request shall be completed by any—

21 (A) large data holder within 45 days of
22 verification of such request from an individual;

23 (B) covered entity that is not considered a
24 large data holder or a covered entity described

1 in section 209 within 60 days of verification of
2 such request from an individual; or

3 (C) covered entity as described in section
4 209 within 90 days of verification of such re-
5 quest from an individual.

6 (2) A response period set forth in this sub-
7 section may be extended once by 45 additional days
8 when reasonably necessary, considering the com-
9 plexity and number of the individual's requests, so
10 long as the covered entity informs the individual of
11 any such extension within the initial 45-day response
12 period, together with the reason for the extension.

13 (d) FREQUENCY AND COST OF ACCESS.—A covered
14 entity—

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

18 (2) with respect to—

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

23 (B) any time beyond the initial 2 times de-
24 scribed in subparagraph (A), may allow the in-

1 dividual to exercise such right for a reasonable
2 fee for each request.

3 (e) VERIFICATION AND EXCEPTIONS.—

4 (1) REQUIRED EXCEPTIONS.—A covered entity
5 shall not permit an individual to exercise a right de-
6 scribed in subsection (a), in whole or in part, if the
7 covered entity—

8 (A) cannot reasonably verify that the indi-
9 vidual making the request to exercise the right
10 is the individual whose covered data is the sub-
11 ject of the request or an individual authorized
12 to make such a request on the individual's be-
13 half;

14 (B) reasonably believes that the request is
15 made to interfere with a contract between the
16 covered entity and another individual;

17 (C) determines that the exercise of the
18 right would require access to or correction of
19 another individual's sensitive covered data; or

20 (D) reasonably believes that the exercise of
21 the right would require the covered entity to en-
22 gage in an unfair or deceptive practice under
23 section 5 of the Federal Trade Commission Act
24 (15 U.S.C. 45).

1 (2) ADDITIONAL INFORMATION.—If a covered
2 entity cannot reasonably verify that a request to ex-
3 ercise a right described in subsection (a) is made by
4 the individual whose covered data is the subject of
5 the request (or an individual authorized to make
6 such a request on the individual’s behalf), the cov-
7 ered entity—

8 (A) may request that the individual mak-
9 ing the request to exercise the right provide any
10 additional information necessary for the sole
11 purpose of verifying the identity of the indi-
12 vidual; and

13 (B) shall not process or transfer such addi-
14 tional information for any other purpose.

15 (3) PERMISSIVE EXCEPTIONS.—

16 (A) IN GENERAL.—A covered entity may
17 decline to comply with a request to exercise a
18 right described in subsection (a), in whole or in
19 part, that would—

20 (i) require the covered entity to retain
21 any covered data collected for a single,
22 one-time transaction, if such covered data
23 is not processed or transferred by the cov-
24 ered entity for any purpose other than
25 completing such transaction;

1 (ii) be impossible or demonstrably im-
2 practicable to comply with, and the covered
3 entity shall provide a description to the re-
4 questor detailing the inability to comply
5 with the request;

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

8 (iv) result in the release of trade se-
9 crets, or other privileged, or confidential
10 business information;

11 (v) require the covered entity to cor-
12 rect any covered data that cannot be rea-
13 sonably verified as being inaccurate or in-
14 complete;

15 (vi) interfere with law enforcement,
16 judicial proceedings, investigations, or rea-
17 sonable efforts to guard against, detect, or
18 investigate malicious or unlawful activity,
19 or enforce valid contracts;

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

24 (viii) prevent a covered entity from
25 being able to maintain a confidential

1 record of deletion requests, maintained
2 solely for the purpose of preventing cov-
3 ered data of an individual who has sub-
4 mitted a deletion request and requests that
5 the covered entity no longer collect, proc-
6 ess, or transfer such data;

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

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.

8 (B) PARTIAL COMPLIANCE.—In a cir-
9 cumstance that would allow a denial pursuant
10 to paragraph (A), a covered entity shall par-
11 tially comply with the remainder of the request
12 if it is possible and not unduly burdensome to
13 do so.

14 (C) NUMBER OF REQUESTS.—For pur-
15 poses of this paragraph, the receipt of a large
16 number of verified requests, on its own, shall
17 not be considered to render compliance with a
18 request demonstrably impossible.

19 (D) FURTHER EXCEPTIONS.—The Com-
20 mission may, by regulation as described in sub-
21 section (f), establish additional permissive ex-
22 ceptions necessary to protect the rights of indi-
23 viduals, alleviate undue burdens on covered en-
24 tities, prevent unjust or unreasonable outcomes
25 from the exercise of access, correction, deletion,

1 or portability rights, or as otherwise necessary
2 to fulfill the purposes of this section. In cre-
3 ating such exceptions, the Commission should
4 consider any relevant changes in technology,
5 means for protecting privacy and other rights,
6 and beneficial uses of covered data by covered
7 entities.

8 (f) REGULATIONS.—Within two years of the date of
9 enactment of this Act, the Commission may promulgate
10 regulations, pursuant to section 553 of title 5, United
11 States Code (5 U.S.C. 553), as necessary to establish
12 processes by which covered entities are to comply with the
13 provisions of this section. Such regulations shall take into
14 consideration—

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

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

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

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

4 (g) ACCESSIBILITY.—A covered entity shall facilitate
5 the ability for individuals to make requests under this sec-
6 tion in any of the ten languages with the most users in
7 the United States, according to the most recent U.S. Cen-
8 sus, if the covered entity provides service in such language.
9 The mechanisms by which a covered entity enables individ-
10 uals to make requests under this section shall be readily
11 accessible and usable by with disabilities.

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

13 (a) WITHDRAWAL OF CONSENT.—A covered entity
14 shall provide an individual with a clear and conspicuous,
15 easy-to-execute means to withdraw any affirmative express
16 consent previously provided by the individual that is as
17 easy to execute by a reasonable individual as the means
18 to provide consent, with respect to the processing or trans-
19 fer of the covered data of the individual.

20 (b) RIGHT TO OPT OUT OF COVERED DATA TRANS-
21 FERS.—

22 (1) IN GENERAL.—A covered entity—

23 (A) shall not transfer the covered data of
24 an individual to a third party if the individual
25 objects to the transfer; and

1 (B) shall allow an individual to object to
2 such transfer through an opt-out mechanism, as
3 described in section 210, if applicable.

4 (2) EXCEPTION.—An individual may not opt
5 out of the collection, processing, and transfer of cov-
6 ered data made pursuant to the exceptions in section
7 101(b)(1) through (11) of this Act.

8 (c) RIGHT TO OPT OUT OF TARGETED ADVER-
9 TISING.—A covered entity that engages in targeted adver-
10 tising shall—

11 (1) prior to engaging in such targeted adver-
12 tising and at all times thereafter, provide an indi-
13 vidual with a clear and conspicuous means to opt
14 out of targeted advertising;

15 (2) abide by such opt-out designations by an in-
16 dividual; and

17 (3) allow an individual to prohibit such targeted
18 advertising through an opt-out mechanism, as de-
19 scribed in section 210, if applicable.

20 (d) INDIVIDUAL AUTONOMY.—A covered entity shall
21 not condition, effectively condition, attempt to condition,
22 or attempt to effectively condition the exercise of any indi-
23 vidual rights under this section through—

1 (1) through the use of any false, fictitious,
2 fraudulent, or materially misleading statement or
3 representation; or

4 (2) the design, modification, or manipulation of
5 any user interface with the purpose or substantial
6 effect of obscuring, subverting, or impairing a rea-
7 sonable individual's autonomy, decision making, or
8 choice to exercise any such rights.

9 **SEC. 205. DATA PROTECTIONS FOR CHILDREN AND MI-**
10 **NORS.**

11 (a) PROHIBITION ON TARGETED ADVERTISING TO
12 CHILDREN AND MINORS.—A covered entity shall not en-
13 gage in targeted advertising to any individual under the
14 age of 17 if the covered entity knows that the individual
15 is under the age of 17.

16 (b) DATA TRANSFER REQUIREMENTS RELATED TO
17 MINORS.—A covered entity shall not transfer the covered
18 data of an individual to a third party without affirmative
19 express consent from the individual or the individual's par-
20 ent or guardian if the covered entity knows that the indi-
21 vidual under the age of 17.

22 (c) KNOWLEDGE .—The knowledge requirement in
23 paragraphs (a) and (b), shall not be construed to require
24 the affirmative collection or processing of any data with
25 respect to the age of an individual or a proxy thereof, or

1 to require that a covered entity implement an age gating
2 regime. Rather, the determination of whether an indi-
3 vidual is under 17 shall be based on the covered data col-
4 lected directly from an individual or a proxy thereof that
5 the covered entity would otherwise collect in the normal
6 course of business.

7 (d) YOUTH PRIVACY AND MARKETING DIVISION.—

8 (1) ESTABLISHMENT.—There is established
9 within the Commission a division to be known as the
10 “Youth Privacy and Marketing Division” (in this
11 section referred to as the “Division”).

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

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

18 (A) the privacy of children and minors;

19 and

20 (B) marketing directed at children and mi-
21 nors.

22 (4) STAFF.—The Director of the Division shall
23 hire adequate staff to carry out the duties described
24 in paragraph (3), including by hiring individuals who

1 are experts in data protection, digital advertising,
2 data analytics, and youth development.

3 (5) REPORTS.—Not later than 1 year after the
4 date of enactment of this Act, and annually there-
5 after, the Commission shall submit to the Committee
6 on Commerce, Science, and Transportation of the
7 Senate and the Committee on Energy and Com-
8 merce of the House of Representatives a report that
9 includes—

10 (A) a description of the work of the Divi-
11 sion regarding emerging concerns relating to
12 youth privacy and marketing practices; and

13 (B) an assessment of how effectively the
14 Division has, during the period for which the
15 report is submitted, assisting the Commission
16 to address youth privacy and marketing prac-
17 tices.

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

22 (e) REPORT BY THE INSPECTOR GENERAL.—

23 (1) IN GENERAL.—Not later than 2 years after
24 the date of enactment of this Act, and biennially
25 thereafter, the Inspector General of the Commission

1 shall submit to the Commission and to the Com-
2 mittee on Commerce, Science, and Transportation of
3 the Senate and the Committee on Energy and Com-
4 merce of the House of Representatives a report re-
5 garding the safe harbor provisions in section 1307 of
6 the Children’s Online Privacy Protection Act of
7 1998 (15 U.S.C. 6503), which shall include—

8 (A) an analysis of whether the safe harbor
9 provisions are—

10 (i) operating fairly and effectively;

11 and

12 (ii) effectively protecting the interests
13 of children and minors; and

14 (B) any proposal or recommendation for
15 policy changes that would improve the effective-
16 ness of the safe harbor provisions.

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

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

22 (a) NOTICE.—Each third-party collecting entity shall
23 place a clear and conspicuous notice on the website or mo-
24 bile application of the third-party collecting entity (if the

1 third-party collecting entity maintains such a website or
2 mobile application) that—

3 (1) notifies individuals that the entity is a
4 third-party collecting entity using specific language
5 that the Commission shall develop through rule-
6 making under section 553 of title 5, United States
7 Code; and

8 (2) includes a link to the website established
9 under subsection (b)(3).

10 (b) THIRD-PARTY COLLECTING ENTITY REGISTRA-
11 TION.—

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

20 (2) REGISTRATION REQUIREMENTS.—In reg-
21 istering with the Commission as required under
22 paragraph (1), a third-party collecting entity shall
23 do the following:

24 (A) Pay to the Commission a registration
25 fee of \$100.

1 (B) Provide the Commission with the fol-
2 lowing information:

3 (i) The legal name and primary phys-
4 ical, email, and internet addresses of the
5 third-party collecting entity.

6 (ii) A description of the categories of
7 data the third-party collecting entity proc-
8 esses and transfers.

9 (iii) The contact information of the
10 third-party collecting entity, including a
11 contact person, telephone number, an e-
12 mail address, a website, and a physical
13 mailing address.

14 (iv) Link to a website through which
15 an individual may easily exercise the rights
16 provided under this subsection.

17 (3) THIRD-PARTY COLLECTING ENTITY REG-
18 ISTRY.—The Commission shall establish and main-
19 tain on a website a searchable, publicly available,
20 central registry of third-party collecting entities that
21 are registered with the Commission under this sub-
22 section that includes the following:

23 (A) A listing of all registered third-party
24 collecting entities and a search feature that al-

1 lows members of the public to identify indi-
2 vidual third-party collecting entities.

3 (B) For each registered third-party col-
4 lecting entity, the information described in
5 paragraph (2).

6 (C) A “Do Not Collect” registry link and
7 mechanism by which an individual may, after
8 the Commission has verified the identity of the
9 individual or individual’s parent or guardian,
10 which may include tokenization, easily submit a
11 request to all registered third-party collecting
12 entities that are not consumer reporting agen-
13 cies, and to the extent they are not acting as
14 consumer reporting agencies, as defined in sec-
15 tion 603(f) of the Fair Credit Reporting Act
16 (15 U.S.C. 1681a(f)) to—

17 (i) delete all covered data related to
18 such individual that the third-party col-
19 lecting entity did not collect from the indi-
20 vidual directly or when acting as a service
21 provider; and

22 (ii) ensure that any third-party col-
23 lecting entity no longer collects covered
24 data related to such individual without the
25 affirmative express consent of such indi-

1 vidual, except insofar as such covered enti-
2 ty is acting as a service provider. Each
3 third-party collecting entity that receives
4 such a request from an individual shall de-
5 lete all the covered data of the individual
6 not later than 30 days after the request is
7 received by the third-party collecting enti-
8 ty.

9 (c) PENALTIES.—A third-party collecting entity that
10 fails to register or provide the notice as required under
11 this section shall be liable for—

12 (1) a civil penalty of \$50 for each day it fails
13 to register or provide notice as required under this
14 subsection, not to exceed a total of \$10,000 for any
15 year; and

16 (2) an amount equal to the registration fees
17 due under paragraph (2) of subsection (b) for each
18 year that it failed to register as required under para-
19 graph (1) of such subsection.

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

21 (a) CIVIL RIGHTS PROTECTIONS.—

22 (1) IN GENERAL.—A covered entity or a service
23 provider may not collect, process, or transfer covered
24 data in a manner that discriminates in or otherwise
25 makes unavailable the equal enjoyment of goods or

1 services on the basis of race, color, religion, national
2 origin, sex, or disability.

3 (2) EXCEPTIONS.—This subsection shall not
4 apply to—

5 (A) the collection, processing, or transfer
6 of covered data for the purpose of—

7 (i) a covered entity's or a service pro-
8 vider's self-testing to prevent or mitigate
9 unlawful discrimination; or

10 (ii) diversifying an applicant, partici-
11 pant, or customer pool; or

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

15 (b) FTC ENFORCEMENT ASSISTANCE.—

16 (1) IN GENERAL.—Whenever the Commission
17 obtains information that a covered entity or service
18 provider may have collected, processed, or trans-
19 ferred covered data in violation of subsection (a), the
20 Commission shall transmit such information as al-
21 lowable under Federal law to any Executive agency
22 with authority to initiate enforcement actions or pro-
23 ceedings relating to such violation.

24 (2) ANNUAL REPORT.—Not later than 3 years
25 after the date of enactment of this Act, and annually

1 thereafter, the Commission shall submit to Congress
2 a report that includes a summary of—

3 (A) the types of information the Commis-
4 sion transmitted to Federal agencies under
5 paragraph (1) during the previous 1-year pe-
6 riod; and

7 (B) how such information relates to Fed-
8 eral civil rights laws.

9 (3) TECHNICAL ASSISTANCE.—In transmitting
10 information under paragraph (1), the Commission
11 may consult and coordinate with, and provide tech-
12 nical and investigative assistance, as appropriate, to
13 such Executive agency.

14 (4) COOPERATION WITH OTHER AGENCIES.—
15 The Commission may implement this subsection by
16 executing agreements or memoranda of under-
17 standing with the appropriate Federal agencies.

18 (c) ALGORITHM IMPACT AND EVALUATION.—

19 (1) ALGORITHM IMPACT ASSESSMENT.—

20 (A) IMPACT ASSESSMENT.—Notwith-
21 standing any other provision of law, not later
22 than 2 years after the date of enactment of this
23 Act, and annually thereafter, a large data hold-
24 er that uses an algorithm that may cause po-
25 tential harm to an individual, and uses such al-

1 algorithm solely or in part, to collect, process or
2 transfer covered data must conduct an impact
3 assessment of such algorithm in accordance
4 with subparagraph (B).

5 (B) IMPACT ASSESSMENT SCOPE.—The im-
6 pact assessment required under subparagraph
7 (A) shall provide the following:

8 (i) A detailed description of the design
9 process and methodologies of the algo-
10 rithm.

11 (ii) A statement of the purpose, pro-
12 posed uses, and foreseeable capabilities
13 outside of the articulated proposed use of
14 the algorithm.

15 (iii) A detailed description of the data
16 used by the algorithm, including the spe-
17 cific categories of data that will be proc-
18 essed as input and any data used to train
19 the model that the algorithm relies on.

20 (iv) A description of the outputs pro-
21 duced by the algorithm.

22 (v) An assessment of the necessity
23 and proportionality of the algorithm in re-
24 lation to its stated purpose, including rea-
25 sons for the superiority of the algorithm

1 over nonautomated decision making meth-
2 ods; and

3 (vi) A detailed description of steps the
4 large data holder has taken or will take to
5 mitigate potential harms to individuals, in-
6 cluding potential harms related to—

7 (I) any individual under the age
8 of 17;

9 (II) making or facilitating adver-
10 tising for, or determining access to, or
11 restrictions on the use of housing,
12 education, employment, healthcare, in-
13 surance, or credit opportunities;

14 (III) determining access to, or re-
15 strictions on the use of, any place of
16 public accommodation, particularly as
17 such harms relate to the protected
18 characteristics of individuals, includ-
19 ing race, color, religion, national ori-
20 gin, sex, or disability; or

21 (IV) disparate impact on the
22 basis of individuals' race, color, reli-
23 gion, national origin, sex, or disability
24 status.

1 (2) ALGORITHM DESIGN EVALUATION.—Not-
2 withstanding any other provision of law, not later
3 than 2 years after the date of enactment of this Act,
4 a covered entity or service provider that knowingly
5 develops an algorithm, solely or in part, to collect,
6 process or transfer covered data or publicly available
7 information shall prior to deploying the algorithm in
8 interstate commerce evaluate the design, structure,
9 and inputs of the algorithm, including any training
10 data used to develop the algorithm, to reduce the
11 risk of the potential harms identified under para-
12 graph (1)(B).

13 (3) OTHER CONSIDERATIONS.—

14 (A) FOCUS.—In complying with para-
15 graphs (1) or (2), a covered entity and a service
16 provider may focus the impact assessment or
17 evaluation on any algorithm, or portions of an
18 algorithm, that may reasonably contribute to
19 the risk of the potential harms identified under
20 paragraph (1)(B).

21 (B) EXTERNAL, INDEPENDENT AUDITOR
22 OR RESEARCHER.—To the extent possible, a
23 covered entity and a service provider shall uti-
24 lize an external, independent auditor or re-
25 searcher to conduct an impact assessment

1 under paragraph (1) or an evaluation under
2 paragraph (2).

3 (C) AVAILABILITY.—

4 (i) IN GENERAL.—A covered entity
5 and a service provider—

6 (I) shall, not later than 30 days
7 after completing an impact assess-
8 ment or evaluation, submit the impact
9 assessment and evaluation conducted
10 under paragraphs (1) and (2) to the
11 Commission;

12 (II) shall, upon request, make
13 such impact assessment and evalua-
14 tion available to Congress; and

15 (III) may make a summary of
16 such impact assessment and evalua-
17 tion publicly available in a place that
18 is easily accessible to individuals.

19 (ii) TRADE SECRETS.—Covered enti-
20 ties and service providers must make all
21 submissions under this section to the Com-
22 mission in unredacted form, but a covered
23 entity and a service provider may redact
24 and segregate any trade secrets (as defined
25 in section 1839 of title 18, United States

1 Code) from public disclosure under this
2 subparagraph.

3 (D) ENFORCEMENT.—The Commission
4 may not use any information obtained solely
5 and exclusively through a covered entity or a
6 service provider’s disclosure of information to
7 the Commission in compliance with this section
8 for any purpose other than enforcing this Act,
9 including the study and report provisions in
10 paragraph 6 of this section. This provision shall
11 not preclude the Commission from providing
12 this information to Congress in response to a
13 subpoena or official Congressional request.

14 (4) GUIDANCE.—Not later than 2 years after
15 the date of enactment of this Act, the Commission
16 shall, in consultation with the Secretary of Com-
17 merce, or their respective designees, publish guid-
18 ance regarding compliance with this section.

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

1 (A) shall submit an impact assessment to
2 the Commission under paragraph (3)(C)(i)(I);
3 and

4 (B) may exclude from this subsection any
5 algorithm that presents low or minimal risk for
6 potential for harms to individuals (as identified
7 under paragraph (1)(B)).

8 (6) STUDY AND REPORT.—

9 (A) STUDY.—The Commission, in con-
10 sultation with the Secretary of Commerce or
11 the Secretary's designee, shall conduct a study,
12 to review any impact assessment or evaluation
13 submitted under this paragraph. Such study
14 shall include an examination of—

15 (i) best practices for the assessment
16 and evaluation of algorithms; and

17 (ii) methods to reduce the risk of
18 harm to individuals that may be related to
19 the use of algorithms.

20 (B) REPORT.—

21 (i) INITIAL REPORT.—Not later than
22 3 years after the date of enactment of this
23 Act, the Commission, in consultation with
24 the Secretary of Commerce or the Sec-
25 retary's designee, shall submit to Congress

1 a report containing the results of the study
2 conducted under subsection (a), together
3 with recommendations for such legislation
4 and administrative action as the Commis-
5 sion determines appropriate.

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

12 **SEC. 208. DATA SECURITY AND PROTECTION OF COVERED**
13 **DATA.**

14 (a) ESTABLISHMENT OF DATA SECURITY PRAC-
15 TICES.—

16 (1) IN GENERAL.—A covered entity or service
17 provider shall establish, implement, and maintain
18 reasonable administrative, technical, and physical
19 data security practices and procedures to protect
20 and secure covered data against unauthorized access
21 and acquisition.

22 (2) CONSIDERATIONS.—The reasonable admin-
23 istrative, technical, and physical data security prac-
24 tices required under paragraph (1) shall be appro-
25 priate to—

1 (A) the size and complexity of the covered
2 entity or service provider;

3 (B) the nature and scope of the covered
4 entity or the service provider's collecting, proc-
5 essing, or transferring of covered data;

6 (C) the volume and nature of the covered
7 data collected, processed, or transferred by the
8 covered entity or service provider;

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

11 (E) the current state of the art in adminis-
12 trative, technical, and physical safeguards for
13 protecting such covered data; and

14 (F) the cost of available tools to improve
15 security and reduce vulnerabilities to unauthor-
16 ized access and acquisition of such covered data
17 in relation to the risks and nature of the cov-
18 ered data.

19 (b) SPECIFIC REQUIREMENTS.—The data security
20 practices required under subsection (a) shall include, at
21 a minimum, the following practices:

22 (1) ASSESS VULNERABILITIES.—Identifying
23 and assessing any material internal and external
24 risk to, and vulnerability in, the security of each sys-
25 tem maintained by the covered entity that collects,

1 processes or transfers covered data, or service pro-
2 vider that collects, processes, or transfers covered
3 data on behalf of the covered entity, including unau-
4 thorized access to or risks to such covered data,
5 human vulnerabilities, access rights, and the use of
6 service providers. With respect to large data holders,
7 such activities shall include a plan to receive and re-
8 spond to unsolicited reports of vulnerabilities by any
9 entity or individual.

10 (2) PREVENTIVE AND CORRECTIVE ACTION.—

11 Taking preventive and corrective action designed to
12 mitigate any reasonably foreseeable risks or
13 vulnerabilities to covered data identified by the cov-
14 ered entity or service provider, consistent with the
15 nature of such risk or vulnerability, which may in-
16 clude implementing administrative, technical, or
17 physical safeguards or changes to data security prac-
18 tices or the architecture, installation, or implementa-
19 tion of network or operating software, among other
20 actions.

21 (3) EVALUATION OF PREVENTIVE AND CORREC-

22 TIVE ACTION.—Evaluating and making reasonable
23 adjustments to the safeguards described in para-
24 graph (2) in light of any material changes in tech-
25 nology, internal or external threats to covered data,

1 and the covered entity or service provider's own
2 changing business arrangements or operations.

3 (4) INFORMATION RETENTION AND DIS-
4 POSAL.—Disposing of covered data that is required
5 to be deleted by law or is no longer necessary for the
6 purpose for which the data was collected, processed
7 or transferred, unless an individual has provided af-
8 firmative express consent to such retention. Such
9 disposal shall include destroying, permanently eras-
10 ing, or otherwise modifying the covered data to
11 make such data permanently unreadable or indeci-
12 pherable and unrecoverable to ensure ongoing com-
13 pliance with this section.

14 (5) TRAINING.—Training each employee with
15 access to covered data on how to safeguard covered
16 data and updating such training as necessary.

17 (6) DESIGNATION.—Designating an officer, em-
18 ployee, or employees to maintain and implement
19 such practices.

20 (7) INCIDENT RESPONSE.—Implementing pro-
21 cedures to detect, respond to, or recover from secu-
22 rity incidents or breaches.

23 (c) REGULATIONS.—The Commission may promul-
24 gate in accordance with section 553 of title 5, United

1 States Code, technology-neutral regulations to establish
2 processes for complying with this section.

3 (d) APPLICABILITY OF OTHER INFORMATION SECU-
4 RITY LAWS.—A covered entity that is required to comply
5 with title V of the Gramm-Leach-Bliley Act (15 U.S.C.
6 6801 et seq.) or the Health Information Technology for
7 Economic and Clinical Health Act (42 U.S.C. 17931 et
8 seq.), and is in compliance with the information security
9 requirements of such Act as determined by the enforce-
10 ment authority in such Act, shall be deemed to be in com-
11 pliance with the requirements of this section with respect
12 to any data covered by such information security require-
13 ments.

14 **SEC. 209. SMALL BUSINESS PROTECTIONS.**

15 (a) IN GENERAL.—

16 (1) Any covered entity or service provider that
17 can establish that it met the requirements described
18 in paragraph (2) for the period of the 3 preceding
19 calendar years (or for the period during which the
20 covered entity has been in existence if such period
21 is less than 3 years) shall—

22 (A) be exempt from compliance with sec-
23 tions 203(a)(4), 208(b)(1)–(3), (5)–(7),
24 301(c); and

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

8 (2) EXEMPTION REQUIREMENTS.—The require-
9 ments of this paragraph are, with respect to a cov-
10 ered entity or a service provider and a period, the
11 following:

12 (A) The covered entity or service provider's
13 average annual gross revenues during the pe-
14 riod did not exceed \$41,000,000.

15 (B) The covered entity or service provider,
16 on average, did not annually collect or process
17 the covered data of more than 200,000 individ-
18 uals during the period beyond the purpose of
19 initiating, rendering, billing for, finalizing, com-
20 pleting, or otherwise collecting payment for a
21 requested service or product, so long as all cov-
22 ered data for such purpose is deleted or de-
23 identified within 90 days.

24 (C) The covered entity or service provider
25 did not derive more than 50 percent of its rev-

1 enue from transferring covered data during any
2 year (or part of a year if the covered entity has
3 been in existence for less than 1 year) that oc-
4 curs during the period.

5 (3) DEFINITION.—For purposes of this section,
6 the term “revenue” as it relates to any covered enti-
7 ty that is not organized to carry on business for its
8 own profit or that of their members, means the
9 gross receipts the covered entity received in whatever
10 form from all sources without subtracting any costs
11 or expenses, and includes contributions, gifts,
12 grants, dues or other assessments, income from in-
13 vestments, or proceeds from the sale of real or per-
14 sonal property.

15 (4) JOURNALISM.—Nothing in this Act shall be
16 construed to limit or diminish First Amendment
17 freedoms to gather and publish information guaran-
18 teed under the Constitution.

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

20 For the rights established under sections 204(b) and
21 (c), and section 206(c)(3)(D) not later than 18 months
22 after the date of enactment of this Act, the Commission
23 shall establish one or more acceptable privacy protective,
24 centralized mechanisms, including global privacy signals
25 such as browser or device privacy settings, for individuals

1 to exercise all such rights through a single interface for
2 a covered entity to utilize to allow an individual to make
3 such opt out designations with respect to covered data re-
4 lated to such individual.

5 **TITLE III—CORPORATE**
6 **ACCOUNTABILITY**

7 **SEC. 301. EXECUTIVE RESPONSIBILITY.**

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

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

16 (2) reporting structures to ensure that such
17 certifying officers are involved in, and are respon-
18 sible for, decisions that impact the entity's compli-
19 ance with this Act.

20 (b) REQUIREMENTS.—A certification submitted
21 under subsection (a) shall be based on a review of the ef-
22 fectiveness of a large data holder's internal controls and
23 reporting structures that is conducted by the certifying of-
24 ficers not more than 90 days before the submission of the
25 certification.

1 (c) DESIGNATION OF PRIVACY AND DATA SECURITY
2 OFFICER.—

3 (1) IN GENERAL.—A covered entity and a serv-
4 ice provider shall designate—

5 (A) 1 or more qualified employees as pri-
6 vacy officers; and

7 (B) 1 or more qualified employees (in addi-
8 tion to any employee designated under subpara-
9 graph (A)) as data security officers.

10 (2) REQUIREMENTS FOR OFFICERS.—An em-
11 ployee who is designated by a covered entity or a
12 service provider as a privacy officer or a data secu-
13 rity officer shall, at a minimum—

14 (A) implement a data privacy program and
15 data security program to safeguard the privacy
16 and security of covered data in compliance with
17 the requirements of this Act; and

18 (B) facilitate the covered entity or service
19 provider’s ongoing compliance with this Act.

20 (3) ADDITIONAL REQUIREMENTS FOR LARGE
21 DATA HOLDERS.—A large data holder shall des-
22 ignate at least 1 of the officers described in para-
23 graph (1) of this subsection to report directly to the
24 highest official at the large data holder as a privacy
25 protection officer who shall, in addition to the re-

1 requirements in paragraph (2), either directly or
2 through a supervised designee or designees—

3 (A) establish processes to periodically re-
4 view and update the privacy and security poli-
5 cies, practices, and procedures of the large data
6 holder, as necessary;

7 (B) conduct biennial and comprehensive
8 audits to ensure the policies, practices, and pro-
9 cedures of the large data holder work to ensure
10 the company is in compliance with all applicable
11 laws and ensure such audits are accessible to
12 the Commission upon such request;

13 (C) develop a program to educate and
14 train employees about compliance requirements;

15 (D) maintain updated, accurate, clear, and
16 understandable records of all privacy and data
17 security practices undertaken by the large data
18 holder; and

19 (E) serve as the point of contact between
20 the large data holder and enforcement authori-
21 ties.

22 (d) LARGE DATA HOLDER PRIVACY IMPACT ASSESS-
23 MENTS.—

24 (1) IN GENERAL.—Not later than 1 year after
25 the date of enactment of this Act or 1 year after the

1 date that a covered entity or service provider first
2 meets the definition of large data holder, whichever
3 is earlier, and biennially thereafter, each large data
4 holder shall conduct a privacy impact assessment
5 that weighs the benefits of the large data holder's
6 covered data collecting, processing, and transfer
7 practices against the potential adverse consequences
8 of such 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 large data holder;

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

24 (B) documented in written form and main-
25 tained by the large data holder unless rendered

1 out of date by a subsequent assessment con-
2 ducted under paragraph (1); and

3 (C) approved by the privacy protection offi-
4 cer designated in subsection (c)(3) of the large
5 data holder.

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

13 **SEC. 302. SERVICE PROVIDERS AND THIRD PARTIES.**

14 (a) **SERVICE PROVIDERS.**—A service provider—

15 (1) shall only collect, process, and transfer serv-
16 ice provider data to the extent strictly necessary and
17 proportionate to provide a service requested by the
18 covered entity. This paragraph shall not require a
19 service provider to collect or process covered data if
20 the service provider would not otherwise do so;

21 (2) shall not collect, process, or transfer service
22 provider data if the service provider has actual
23 knowledge that the covered entity violated this Act
24 with respect to such data;

1 (3) shall assist a covered entity in fulfilling the
2 covered entity's obligation to respond to individual
3 rights requests pursuant to section 203, by appropriate technical and organizational measures, taking
4 into account the nature of the processing and the information reasonably available to the service provider;
5
6
7

8 (4) may engage another service provider for
9 purposes of processing service provider data on behalf of a covered entity only after providing the covered
10 entity that is directing the services or functions of the service provider with respect to such service
11 provider data with notice, and pursuant to a written contract that requires such other service provider to
12 satisfy the obligations of the service provider with respect to such service provider data;
13
14
15
16

17 (5) shall upon the reasonable request of the
18 covered entity, make available to the covered entity information necessary to demonstrate the service
19 provider's compliance with the obligations in this Act, which may include making available a report of
20 an independent assessment arranged by the service provider on terms agreed to by the parties and making
21 the report required under section 207(c)(2) as applicable;
22
23
24
25

1 (6) shall, at the covered entity's direction, de-
2 lete or return all covered data to the covered entity
3 as requested at the end of the provision of services,
4 unless retention of the covered data is required by
5 law;

6 (7) shall not transfer service provider data to
7 any person with the exception of another service pro-
8 vider without the affirmative express consent, ob-
9 tained by the covered entity with the direct relation-
10 ship to the individual that is directing the services
11 or functions of the service provider with respect to
12 the service provider data, of the individual to whom
13 the service provider data is linked or reasonably
14 linkable;

15 (8) shall develop, implement, and maintain rea-
16 sonable administrative, technical, and physical safe-
17 guards that are designed to protect the security and
18 confidentiality of covered data it processes consistent
19 with section 208; and

20 (9) shall be exempt from the requirements of
21 section 202(d) with respect to service provider data
22 but shall provide direct notification regarding mate-
23 rial changes to its privacy policy to each covered en-
24 tity with which it provides services or functions as
25 a service provider, in each language that the privacy

1 policy is made available. Compliance with this provi-
2 sion does not alleviate any obligations the service
3 provider has to the covered entity to which it pro-
4 vides services or functions as a service provider.

5 (b) CONTRACTS BETWEEN COVERED ENTITIES AND
6 SERVICE PROVIDERS.—A person or entity may act as a
7 service provider pursuant to a written contract between
8 the covered entity and the service provider, or a written
9 contract between one service provider and a second service
10 provider as permitted in section 302(a)(4), provided that
11 the contract—

12 (1) governs the service provider’s data proc-
13 essing procedures with respect to processing or
14 transfer performed on behalf of the covered entity or
15 service provider;

16 (2) clearly sets forth—

17 (A) instructions for processing data;

18 (B) the nature and purpose of processing;

19 (C) the type of data subject to processing;

20 (D) the duration of processing; and

21 (E) the rights and obligations of both par-

22 ties; and

23 (3) does not relieve a covered entity or a service
24 provider of an obligation under this Act; and

25 (4) prohibits—

1 (A) collecting, processing, or transferring
2 covered data in contravention to subsection (a);
3 and

4 (B) combining service provider data with
5 covered data which the service provider receives
6 from or on behalf of another person or persons
7 or collects from its own interaction with an in-
8 dividual. The contract may, subject to agree-
9 ment with the service provider, permit a covered
10 entity to monitor the service provider's compli-
11 ance with the contract through measures in-
12 cluding, but not limited to, ongoing manual re-
13 views and automated scans, and regular assess-
14 ments, audits, or other technical and oper-
15 ational testing at least once every 12 months.

16 (c) RELATIONSHIP BETWEEN COVERED ENTITIES
17 AND SERVICE PROVIDERS.—

18 (1) Determining whether a person is acting as
19 a covered entity or service provider with respect to
20 a specific processing of data is a fact-based deter-
21 mination that depends upon the context in which
22 such data is processed.

23 (2) A covered entity or service provider that
24 transfers covered data to a service provider, in com-
25 pliance with the requirements of this Act, is not lia-

1 ble for a violation of this Act by the service provider
2 to whom such covered data was transferred, this Act
3 provided that, at the time of transferring such cov-
4 ered data, the covered entity or service provider did
5 not know or have reason to know that the service
6 provider would likely commit a violation of this Act.

7 (3) A covered entity or service provider that re-
8 ceives covered data in compliance with the require-
9 ments of this Act is not in violation of this Act as
10 a result of a violation by a covered entity or service
11 provider from which it receives such covered data.

12 (d) THIRD PARTIES.—A third party—

13 (1) shall not process third party data for a
14 processing purpose other than, in the case of sen-
15 sitive covered data, the processing purpose for which
16 the individual gave affirmative express consent and,
17 in the case of non-sensitive data, the processing pur-
18 pose for which the covered entity made a disclosure
19 pursuant to section 204(b)(4);

20 (2) for purposes of paragraph (1), may reason-
21 ably rely on representations made by the covered en-
22 tity that transferred the third party data , provided
23 that the third party conducts reasonable due dili-
24 gence on the representations of the covered entity
25 and finds those representations to be credible; and

1 (3) shall be exempt from the requirements of
2 section 204 with respect to third party data, but
3 shall otherwise have the same responsibilities and
4 obligations as a covered entity with respect to such
5 data under all other provisions of this Act.

6 (e) **ADDITIONAL OBLIGATIONS ON COVERED ENTI-**
7 **TIES.—**

8 (1) **IN GENERAL.—**A covered entity or service
9 provider shall exercise reasonable due diligence in—
10 (A) selecting a service provider; and
11 (B) deciding to transfer covered data to a
12 third party.

13 (2) **GUIDANCE.—**Not later than 2 years after
14 the date of enactment of this Act, the Commission
15 shall publish guidance regarding compliance with
16 this subsection, taking into consideration the bur-
17 dens on small- and medium-sized covered entities.

18 **SEC. 303. TECHNICAL COMPLIANCE PROGRAMS.**

19 (a) **IN GENERAL.—**Not later than 1 year after the
20 date of the enactment of this Act, the Commission shall
21 promulgate regulations under section 553 of title 5,
22 United States Code, to establish a process for the proposal
23 and approval of technical compliance programs under this
24 section specific to any technology, product, service, or

1 method used by a covered entity to collect, process, or
2 transfer covered data.

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

7 (1) establish guidelines for compliance with this
8 Act;

9 (2) meet or exceed the requirements of this Act;
10 and

11 (3) be made publicly available to any individual
12 whose covered data is collected, processed, or trans-
13 ferred using such technology, product, service, or
14 method.

15 (c) APPROVAL PROCESS.—

16 (1) IN GENERAL.—Any request for approval,
17 amendment, or repeal of a technical compliance pro-
18 gram may be submitted to the Commission by any
19 person, including a covered entity, a representative
20 of a covered entity, an association of covered enti-
21 ties, or a public interest group or organization.
22 Within 90 days, the Commission shall publish the
23 request and provide an opportunity for public com-
24 ment on the proposal.

1 (2) EXPEDITED RESPONSE TO REQUESTS.—Be-
2 ginning 1 year after the date of enactment of this
3 Act, the Commission shall act upon a request for the
4 proposal and approval of a technical compliance pro-
5 gram not later than 180 days after the filing of the
6 request, and shall set forth publicly in writing its
7 conclusions with regard to such request.

8 (d) RIGHT TO APPEAL.—Final action by the Com-
9 mission on a request for approval, amendment, or repeal
10 of a technical compliance program, or the failure to act
11 within the 180 day period after a request for approval,
12 amendment, or repeal of a technical compliance program
13 is made under subsection (c), may be appealed to a Fed-
14 eral district court of the United States of appropriate ju-
15 risdiction as provided for in section 702 of title 5, United
16 States Code.

17 (e) EFFECT ON ENFORCEMENT.—

18 (1) IN GENERAL.—Prior to commencing an in-
19 vestigation or enforcement action against any cov-
20 ered entity under this Act, the Commission and
21 state Attorney General shall consider the covered en-
22 tity’s history of compliance with any technical com-
23 pliance program approved under this section and
24 any action taken by the covered entity to remedy
25 noncompliance with such program. If such enforce-

1 ment action described in Sec. 403 is commenced, the
2 covered entity's history of compliance with any tech-
3 nical compliance program approved under this sec-
4 tion and any action taken by the covered entity to
5 remedy noncompliance with such program shall be
6 taken into consideration when determining liability
7 or a penalty. The covered entity's history of compli-
8 ance with any technical compliance program shall
9 not affect any burden of proof or the weight given
10 to evidence in an enforcement or judicial proceeding.

11 (2) COMMISSION AUTHORITY.—Approval of a
12 technical compliance program shall not limit the au-
13 thority of the Commission, including the Commis-
14 sion's authority to commence an investigation or en-
15 forcement action against any covered entity under
16 this Act or any other Act.

17 (3) RULE OF CONSTRUCTION.—Nothing in this
18 subsection shall provide any individual, class of indi-
19 viduals, or person with any right to seek discovery
20 of any non-public Commission deliberations or activi-
21 ties or impose any pleading requirement on the
22 Commission should it bring an enforcement action of
23 any kind.

1 **SEC. 304. COMMISSION APPROVED COMPLIANCE GUIDE-**
2 **LINES.**

3 (a) APPLICATION FOR COMPLIANCE GUIDELINE AP-
4 PROVAL.—

5 (1) IN GENERAL.—A covered entity that is not
6 a third-party collecting entity and meets the require-
7 ments of section 209, or a group of such covered en-
8 tities, may apply to the Commission for approval of
9 1 or more sets of compliance guidelines governing
10 the collection, processing, and transfer of covered
11 data by the covered entity or group of covered enti-
12 ties.

13 (2) APPLICATION REQUIREMENTS.—Such appli-
14 cation shall include—

15 (A) a description of how the proposed
16 guidelines will meet or exceed the requirements
17 of this Act;

18 (B) a description of the entities or activi-
19 ties the proposed set of compliance guidelines is
20 designed to cover;

21 (C) a list of the covered entities that meet
22 the requirements of section 209 and are not
23 third-party collecting entities, if any are known
24 at the time of application, that intend to adhere
25 to the compliance guidelines; and

1 (D) a description of how such covered enti-
2 ties will be independently assessed for adher-
3 ence to such compliance guidelines, including
4 the independent organization not associated
5 with any of the covered entities that may par-
6 ticipate in guidelines that will administer such
7 guidelines.

8 (3) COMMISSION REVIEW.—

9 (A) INITIAL APPROVAL.—

10 (i) PUBLIC COMMENT PERIOD.—With-
11 in 90 days after the receipt of proposed
12 guidelines submitted pursuant to para-
13 graph (2), the Commission shall publish
14 the proposal and provide an opportunity
15 for public comment on such compliance
16 guidelines.

17 (ii) APPROVAL.—The Commission
18 shall approve an application regarding pro-
19 posed guidelines under paragraph (2) if
20 the applicant demonstrates that the com-
21 pliance guidelines—

22 (I) meet or exceed requirements
23 of this Act;

24 (II) provide for the regular re-
25 view and validation by an independent

1 organization not associated with any
2 of the covered entities that may par-
3 ticipate in the guidelines and that is
4 approved by the Commission to con-
5 duct such reviews of the compliance
6 guidelines of the covered entity or en-
7 tities to ensure that the covered entity
8 or entities continue to meet or exceed
9 the requirements of this Act; and

10 (III) include a means of enforce-
11 ment if a covered entity does not meet
12 or exceed the requirements in the
13 guidelines, which may include referral
14 to the Commission for enforcement
15 consistent with section 401 or referral
16 to the appropriate State attorney gen-
17 eral for enforcement consistent with
18 section 402.

19 (iii) **TIMELINE.**—Within 1 year of re-
20 ceiving an application regarding proposed
21 guidelines under paragraph (2), the Com-
22 mission shall issue a determination approv-
23 ing or denying the application and pro-
24 viding its reasons for approving or denying
25 such application.

1 (B) APPROVAL OF MODIFICATIONS.—

2 (i) IN GENERAL.—If the independent
3 organization administering a set of guide-
4 lines makes material changes to guidelines
5 previously approved by the Commission,
6 the independent organization must submit
7 the updated guidelines to the Commission
8 for approval. As soon as feasible, the Com-
9 mission shall publish the updated guide-
10 lines and provide an opportunity for public
11 comment.

12 (ii) TIMELINE.—The Commission
13 shall approve or deny any material change
14 to the guidelines within 180 days after re-
15 ceipt of the submission for approval.

16 (b) WITHDRAWAL OF APPROVAL.—If at any time the
17 Commission determines that the guidelines previously ap-
18 proved no longer meet the requirements of this Act or a
19 regulation promulgated under this Act or that compliance
20 with the approved guidelines is insufficiently enforced by
21 the independent organization administering the guidelines,
22 the Commission shall notify the covered entities or group
23 of such entities and the independent organization of its
24 determination to withdraw approval of such guidelines and
25 the basis for doing so. Upon receipt of such notice, the

1 covered entity or group of such entities and the inde-
2 pendent organization may cure any alleged deficiency with
3 the guidelines or the enforcement of such guidelines within
4 180 days and submit the proposed cure or cures to the
5 Commission. If the Commission determines that such
6 cures eliminate the alleged deficiency in the guidelines,
7 then the Commission may not withdraw approval of such
8 guidelines on the basis of such determination.

9 (c) DEEMED COMPLIANCE.—A covered entity that is
10 eligible to participate under subsection (a)(1), and partici-
11 pates, in guidelines approved under this section shall be
12 deemed in compliance with the relevant provisions of this
13 Act if it is in compliance with such guidelines.

14 **SEC. 305. DIGITAL CONTENT FORGERIES.**

15 (a) REPORTS.—Not later than 1 year after the date
16 of enactment of this Act, and annually thereafter, the Sec-
17 retary of Commerce or the Secretary's designee shall pub-
18 lish a report regarding digital content forgeries.

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

21 (1) A definition of digital content forgeries
22 along with accompanying explanatory materials, ex-
23 cept that the definition developed pursuant to this
24 section shall not supersede any other provision of

1 law or be construed to limit the authority of any ex-
2 ecutive agency related to digital content forgeries.

3 (2) A description of the common sources of dig-
4 ital content forgeries in the United States and com-
5 mercial sources of digital content forgery tech-
6 nologies.

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

9 (4) An analysis of the methods and standards
10 available to identify digital content forgeries as well
11 as a description of the commercial technological
12 counter-measures that are, or could be, used to ad-
13 dress concerns with digital content forgeries, which
14 may include the provision of warnings to viewers of
15 suspect content.

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

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

1 **TITLE IV—ENFORCEMENT, AP-**
2 **PLICABILITY, AND MISCELLA-**
3 **NEOUS**

4 **SEC. 401. ENFORCEMENT BY THE FEDERAL TRADE COM-**
5 **MISSION.**

6 (a) NEW BUREAU.—

7 (1) IN GENERAL.—The Commission shall estab-
8 lish within the Commission a new bureau, the Bu-
9 reau of Privacy, which shall be comparable in struc-
10 ture, size, organization, and authority to the existing
11 Bureaus within the Commission related to consumer
12 protection and competition.

13 (2) MISSION.—The mission of the bureau es-
14 tablished under this subsection shall be to assist the
15 Commission in exercising the Commission's author-
16 ity under this Act and related authorities.

17 (3) TIMELINE.—The bureau shall be estab-
18 lished, staffed, and fully operational not later than
19 1 year after the date of enactment of this Act.

20 (b) OFFICE OF BUSINESS MENTORSHIP.—The Direc-
21 tor of the Bureau established under subsection (a) shall
22 establish within the Bureau an Office of Business
23 Mentorship to provide guidance and education to covered
24 entities regarding compliance with this Act. Covered enti-
25 ties may request advice from the Commission or this office

1 with respect to a course of action which the covered entity
2 proposes to pursue and which may relate to the require-
3 ments of this Act.

4 (c) ENFORCEMENT BY THE FEDERAL TRADE COM-
5 MISSION.—

6 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
7 TICES.—A violation of this Act or a regulation pro-
8 mulgated under this Act shall be treated as a viola-
9 tion of a rule defining an unfair or deceptive act or
10 practice prescribed under section 18(a)(1)(B) of the
11 Federal Trade Commission Act (15 U.S.C.
12 57a(a)(1)(B)).

13 (2) POWERS OF THE COMMISSION.—

14 (A) IN GENERAL.—Except as provided in
15 paragraphs (3), (4), and (5), the Commission
16 shall enforce this Act and the regulations pro-
17 mulgated under this Act in the same manner,
18 by the same means, and with the same jurisdic-
19 tion, powers, and duties as though all applicable
20 terms and provisions of the Federal Trade
21 Commission Act (15 U.S.C. 41 et seq.) were in-
22 corporated into and made a part of this Act.

23 (B) PRIVILEGES AND IMMUNITIES.—Any
24 person who violates this Act or a regulation
25 promulgated under this Act shall be subject to

1 the penalties and entitled to the privileges and
2 immunities provided in the Federal Trade Com-
3 mission Act (15 U.S.C. 41 et seq.).

4 (3) LIMITING CERTAIN ACTIONS UNRELATED
5 TO THIS ACT.—If the Commission brings a civil ac-
6 tion under this Act alleging that an act or practice
7 violates this Act or a regulation promulgated under
8 this Act, the Commission may not seek a cease and
9 desist order against the same defendant under sec-
10 tion 5(b) of the Federal Trade Commission Act (15
11 U.S.C. 45(b)) to stop that same act or practice on
12 the grounds that such act or practice constitutes an
13 unfair or deceptive act or practice.

14 (4) COMMON CARRIERS AND NONPROFITS.—
15 Notwithstanding any jurisdictional limitation of the
16 Commission with respect to consumer protection or
17 privacy, the Commission shall enforce this Act and
18 the regulations promulgated under this Act, in the
19 same manner provided in subsections (1), (2), (3),
20 and (5) of this subsection, with respect to common
21 carriers subject to the Communications Act of 1934
22 (47 U.S.C. 151 et seq) and All Acts amendatory
23 thereof and supplementary thereto; and organiza-
24 tions not organized to carry on business for their
25 own profit or that of their members.

1 (5) DATA PRIVACY AND SECURITY VICTIMS RE-
2 LIEF FUND.—

3 (A) ESTABLISHMENT OF VICTIMS RELIEF
4 FUND.—There is established in the Treasury of
5 the United States a separate fund to be known
6 as the “Privacy and Security Victims Relief
7 Fund” (referred to in this paragraph as the
8 “Victims Relief Fund”).

9 (B) DEPOSITS.—

10 (i) DEPOSITS.—The amount of any
11 civil penalty obtained against any covered
12 entity or service provider or any other re-
13 lief ordered to provide redress, payments
14 or compensation, or other monetary relief
15 to individuals that cannot be located or the
16 payment of which would otherwise not be
17 practicable in any judicial or administra-
18 tive action to enforce this Act or a regula-
19 tion promulgated under this Act shall be
20 deposited into the Victims Relief Fund.

21 (C) USE OF FUND AMOUNTS.—

22 (i) AVAILABILITY TO THE COMMIS-
23 SION.—Notwithstanding section 3302 of
24 title 31, United States Code, amounts in
25 the Victims Relief Fund shall be available

1 to the Commission, without fiscal year lim-
2 itation, to provide redress, payments or
3 compensation, or other monetary relief to
4 individuals affected by an act or practice
5 for which relief has been obtained under
6 this Act.

7 (ii) OTHER PERMISSIBLE USES.—To
8 the extent that individuals cannot be lo-
9 cated or such redress, payments or com-
10 pensation, or other monetary relief are oth-
11 erwise not practicable, the Commission
12 may use such funds for the purpose of—

13 (I) funding the activities of the
14 Office of Business Mentorship estab-
15 lished under subsection (b); or

16 (II) engaging in technological re-
17 search that the Commission considers
18 necessary to enforce or administer
19 this Act.

20 **SEC. 402. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

21 (a) CIVIL ACTION.—In any case in which the attor-
22 ney general of a State or State Privacy Authority has rea-
23 son to believe that an interest of the residents of that state
24 has been, may be, or is adversely affected by the engage-
25 ment of any a covered entity or service provider in an act

1 or practice that has violated this Act or a regulation pro-
2 mulgated under this Act, the attorney general of the State,
3 or State Privacy Authority, may bring a civil action in the
4 name of the State, or as *parens patriae* on behalf of the
5 residents of the State. Any such action shall be brought
6 exclusively in an appropriate Federal district court of the
7 United States to—

8 (1) enjoin that act or practice;

9 (2) enforce compliance with this Act or the reg-
10 ulation;

11 (3) obtain damages, civil penalties, restitution,
12 or other compensation on behalf of the residents of
13 the State; or

14 (4) reasonable attorneys' fees and other litiga-
15 tion costs reasonably incurred.

16 (b) RIGHTS OF THE COMMISSION.—

17 (1) IN GENERAL.—Except where not feasible,
18 the attorney general of a State or State Privacy Au-
19 thority shall notify the Commission in writing prior
20 to initiating a civil action under subsection (a). Such
21 notice shall include a copy of the complaint to be
22 filed to initiate such action. Upon receiving such no-
23 tice, the Commission may intervene in such action as
24 of right pursuant to the Federal Rules of Civil Pro-
25 cedure.

1 (2) NOTIFICATION TIMELINE.—Where it is not
2 feasible for the attorney general of a State or State
3 Privacy Authority to provide the notification re-
4 quired by paragraph (1) before initiating a civil ac-
5 tion under subsection (a), the attorney general of a
6 State or State Privacy Authority shall notify the
7 Commission immediately after initiating the civil ac-
8 tion.

9 (c) ACTIONS BY THE COMMISSION.—In any case in
10 which a civil action is instituted by or on behalf of the
11 Commission for violation of this Act or a regulation pro-
12 mulgated under this Act, no attorney general or State Pri-
13 vacy Authority may, during the pendency of such action,
14 institute a civil action against any defendant named in the
15 complaint in the action instituted by or on behalf of the
16 Commission for violation of this Act or a regulation pro-
17 mulgated under this Act that is alleged in such complaint,
18 if the Commission’s complaint alleges such violations af-
19 fected the residents of the relevant state or individuals na-
20 tionwide. In a case brought by the Commission that af-
21 fects the interests of a State, an attorney general of such
22 state or State Privacy Authority may intervene as of right
23 pursuant to the Federal Rules of Civil Procedure.

24 (d) RULE OF CONSTRUCTION.—Nothing in this sec-
25 tion shall be construed to prevent the attorney general of

1 a State or State Privacy Authority from exercising the
2 powers conferred on the attorney general or State Privacy
3 Authority to conduct investigations, to administer oaths
4 or affirmations, or to compel the attendance of witnesses
5 or the production of documentary or other evidence.

6 (e) PRESERVATION OF STATE POWERS.—Except as
7 provided in subsection (c), no provision of this section
8 shall be construed as altering, limiting, or affecting the
9 authority of a State attorney general or State Privacy Au-
10 thority to—

11 (1) bring an action or other regulatory pro-
12 ceeding arising solely under the laws in effect in that
13 State; or

14 (2) exercise the powers conferred on the attor-
15 ney general or State Privacy Authority by the laws
16 of the State, including the ability to conduct inves-
17 tigation, administer oaths or affirmations, or com-
18 pel the attendance of witnesses or the production of
19 documentary or other evidence.

20 **SEC. 403. ENFORCEMENT BY PERSONS.**

21 (a) ENFORCEMENT BY PERSONS.—

22 (1) IN GENERAL.—Beginning 4 years after the
23 date on which this Act takes effect, any person or
24 class of persons who suffers an injury that could be
25 addressed by the relief permitted in paragraph (2)

1 for a violation of this Act or a regulation promul-
2 gated under this Act by a covered entity may bring
3 a civil action against such entity in any Federal
4 court of competent jurisdiction.

5 (2) RELIEF.—In a civil action brought under
6 paragraph (1) in which a plaintiff prevails, the court
7 may award the plaintiff—

8 (A) an amount equal to the sum of any
9 compensatory damages;

10 (B) injunctive or declaratory relief; and

11 (C) reasonable attorney's fees and litiga-
12 tion costs.

13 (3) RIGHTS OF THE COMMISSION AND STATE
14 ATTORNEYS GENERAL.—

15 (A) IN GENERAL.—Prior to a person or
16 class of persons bringing a civil action under
17 paragraph (1), such person or class of persons
18 must first notify the Commission and the attor-
19 ney general of the State of the persons resi-
20 dence in writing outlining their desire to com-
21 mence a civil action. Upon receiving such no-
22 tice, the Commission and State attorney general
23 shall make a determination and respond to such
24 person or class of persons, not later than 60
25 days after receiving such notice, as to whether

1 they will independently seek to take action, and
2 upon taking action—

3 (i) be heard on all matters arising in
4 such action; and

5 (ii) file petitions for appeal of a deci-
6 sion in such action.

7 (B) BAD FAITH.—Any written communica-
8 tion requesting a monetary payment that is
9 sent to a covered entity shall be considered to
10 have been sent in bad faith and shall be unlaw-
11 ful as defined in this Act, if the written commu-
12 nication was sent:

13 (i) Prior to the date that is 60 days
14 after either a State attorney general or the
15 Commission has received the notice re-
16 quired under subparagraph (A).

17 (ii) After the Commission or attorney
18 general of a State made the determination
19 to independently seek civil actions against
20 such entity as outlined in subparagraph
21 (A).

22 (4) FTC STUDY.—Beginning on the date that
23 is 5 years after the date of enactment of this Act,
24 the Commission's Bureau of Economics shall con-
25 duct an annual study to determine the economic im-

1 pacts in the United States of demand letters sent
2 pursuant to this Act and the scope of the rights of
3 a person to bring forth civil actions against covered
4 entities. Such study shall include, but not be limited
5 to include the following:

6 (A) The impact on increasing insurance
7 rates in the United States.

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

10 (C) The impact on the creation and growth
11 of startup companies, including tech startup
12 companies.

13 (D) Any emerging risks and long-term
14 trends in relevant marketplaces, supply chains,
15 and labor availability.

16 (5) REPORT TO CONGRESS.—Not later than 1
17 year after the first day on which persons and classes
18 of persons are able to bring civil actions under this
19 subsection, and annually thereafter, the Commission
20 shall submit to the Committee on Energy and Com-
21 merce of the House of Representatives and the Com-
22 mittee on Commerce, Science, and Transportation of
23 the Senate a report that contains the results of the
24 study conducted under paragraph (4).

1 (b) PRE-DISPUTE ARBITRATION AGREEMENTS AND
2 PRE-DISPUTE JOINT ACTION WAIVERS.—

3 (1) ARBITRATION.—Notwithstanding any other
4 provision of law, no pre-dispute arbitration agree-
5 ment with respect to an individual under the age of
6 18 may limit any of the rights provided in this Act.

7 (2) JOINT ACTION WAIVERS.—

8 (A) Notwithstanding any other provision of
9 law, no general agreement for pre-dispute joint
10 action waiver with respect to an individual
11 under the age of 18 may limit any of the rights
12 provided in this Act.

13 (B) Notwithstanding any other provision of
14 law, no arbitral or administrative pre-dispute
15 joint action waiver may limit any of the rights
16 provided in this Act irrespective of the age of
17 a party to such agreement.

18 (3) DEFINITIONS.—For purposes of this sub-
19 section:

20 (A) PRE-DISPUTE ARBITRATION AGREE-
21 MENT.—The term “pre-dispute arbitration
22 agreement” means any agreement to arbitrate a
23 dispute that has not arisen at the time of the
24 making of the agreement.

1 (B) GENERAL PRE-DISPUTE JOINT-ACTION
2 WAIVER.—The term “pre-dispute joint-action
3 waiver” means an agreement, whether or not
4 part of a pre-dispute arbitration agreement,
5 that would prohibit or waive the right of 1 of
6 the parties to the agreement to participate in a
7 joint, class, or collective action in a judicial, ar-
8 bitral, administrative, or other related forum,
9 concerning a dispute that has not yet arisen at
10 the time of the making of the agreement.

11 (C) ARBITRAL OR ADMINISTRATIVE PRE-
12 DISPUTE JOINT-ACTION WAIVER.—The term
13 “arbitral or administrative pre-dispute joint-ac-
14 tion waiver” means an agreement, whether or
15 not part of a pre-dispute arbitration agreement,
16 that would prohibit or waive the right of 1 of
17 the parties to the agreement to participate in a
18 joint, class, or collective action in a arbitral, ad-
19 ministrative, or other related forum, concerning
20 a dispute that has not yet arisen at the time of
21 the making of the agreement.

22 (c) RIGHT TO CURE.—

23 (1) NOTICE.—Subject to paragraph (3), with
24 respect to an action under this section for (i) injunc-
25 tive relief; or (ii) an action against a covered entity

1 that meets the requirements of section 209 of this
2 Act, such action may be brought by a person or
3 class of persons if—prior to initiating such action—
4 the person or class of persons provides to the cov-
5 ered entity 45 days’ written notice identifying the
6 specific provisions of this Act the person or class of
7 persons alleges have been or are being violated.

8 (2) EFFECT OF CURE.—Subject to paragraph
9 (3), in the event a cure is possible, if within the 45
10 days the covered entity demonstrates it has cured
11 the noticed violation or violations and provides the
12 person or class of persons an express written state-
13 ment that the violation or violations has been cured
14 and that no further violations shall occur, an action
15 for injunctive relief may be reasonably dismissed.

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

20 (d) DEMAND LETTER.—If a person or class of per-
21 sons sends correspondence to a covered entity alleging a
22 violation of the provisions of this Act and requests a mone-
23 tary payment, such correspondence shall include the fol-
24 lowing language: “Please visit the website of the Federal
25 Trade Commission to understand your rights pursuant to

1 this letter” followed by a hyperlink to the webpage of the
2 Commission required under section 201. If such cor-
3 respondence does not include such language and
4 hyperlink, the person or joint class of persons shall forfeit
5 their rights under this section.

6 (e) APPLICABILITY.—This section shall only apply to
7 any claim alleging a violation of section 102, 104, 202,
8 203, 204, 205(a), 205(b), 206(c)(3)(D), 207(a), 208(a),
9 or 302 for which relief described in subsection (a)(2) may
10 be granted.

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

12 (a) FEDERAL LAW PRESERVATION.—

13 (1) IN GENERAL.—Nothing in this Act or a reg-
14 ulation promulgated under this Act shall be con-
15 strued to limit—

16 (A) the authority of the Commission, or
17 any other Executive agency, under any other
18 provision of law;

19 (B) any requirement for a common carrier
20 subject to section 64.2011 of title 47, Code of
21 Federal Regulations, regarding information se-
22 curity breaches; or

23 (C) any other provision of Federal law un-
24 less specifically authorized by this Act.

1 (2) APPLICABILITY OF OTHER PRIVACY RE-
2 QUIREMENTS.—A covered entity that is required to
3 comply with title V of the Gramm-Leach-Bliley Act
4 (15 U.S.C. 6801 et seq.), the Health Information
5 Technology for Economic and Clinical Health Act
6 (42 U.S.C. 17931 et seq.), part C of title XI of the
7 Social Security Act (42 U.S.C. 1320d et seq.), the
8 Fair Credit Reporting Act (15 U.S.C. 1681 et seq.),
9 the Family Educational Rights and Privacy Act (20
10 U.S.C. 1232g; part 99 of title 34, Code of Federal
11 Regulations), or the regulations promulgated pursu-
12 ant to section 264(e) of the Health Insurance Port-
13 ability and Accountability Act of 1996 (42 U.S.C.
14 1320d–2 note), and is in compliance with the data
15 privacy requirements of such regulations, part, title,
16 or Act (as applicable), shall be deemed to be in com-
17 pliance with the related requirements of this title,
18 except for section 208, solely and exclusively with re-
19 spect to data subject to the requirements of such
20 regulations, part, title, or Act. Not later than 1 year
21 after the date of enactment of this Act, the Commis-
22 sion shall issue guidance describing the implementa-
23 tion of this paragraph.

24 (3) APPLICABILITY OF OTHER DATA SECURITY
25 REQUIREMENTS.—A covered entity that is required

1 to comply with title V of the Gramm-Leach-Bliley
2 Act (15 U.S.C. 6801 et seq.), the Health Informa-
3 tion Technology for Economic and Clinical Health
4 Act (42 U.S.C. 17931 et seq.), part C of title XI of
5 the Social Security Act (42 U.S.C. 1320d et seq.),
6 or the regulations promulgated pursuant to section
7 264(c) of the Health Insurance Portability and Ac-
8 countability Act of 1996 (42 U.S.C. 1320d–2 note),
9 and is in compliance with the information security
10 requirements of such regulations, part, title, or Act
11 (as applicable), shall be deemed to be in compliance
12 with the requirements of section 208 solely and ex-
13 clusively with respect to data subject to the require-
14 ments of such regulations, part, title, or Act. Not
15 later than 1 year after the date of enactment of this
16 Act, the Commission shall issue guidance describing
17 the implementation of this paragraph.

18 (b) PREEMPTION OF STATE LAWS.—

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

1 Act, or a rule, regulation, or requirement promul-
2 gated under this Act.

3 (2) STATE LAW PRESERVATION.—Paragraph
4 (1) shall not be construed to preempt, displace, or
5 supplant the following State laws, rules, regulations,
6 or requirements:

7 (A) Consumer protection laws of general
8 applicability such as laws regulating deceptive,
9 unfair, or unconscionable practices. However,
10 the fact of a violation of this Act shall not be
11 pleaded as an element of any violation of such
12 law.

13 (B) Civil rights laws.

14 (C) Laws that govern the privacy rights or
15 other protections of employees, employee infor-
16 mation, students, or student information.

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

19 (E) Contract or tort law.

20 (F) Criminal laws governing fraud, theft,
21 including identity theft, unauthorized access to
22 information or electronic devices, or unauthor-
23 ized use of information, malicious behavior, or
24 similar provisions, or laws of criminal proce-
25 dure.

1 (G) Criminal or civil laws regarding
2 cyberstalking, cyberbullying, nonconsensual por-
3 nography, or sexual harassment.

4 (H) Public safety or sector specific laws
5 unrelated to privacy or security.

6 (I) Laws that address public records,
7 criminal justice information systems, arrest
8 records, mug shots, conviction records, or non-
9 conviction records.

10 (J) Laws that address banking records, fi-
11 nancial records, tax records, Social Security
12 numbers, credit cards, credit reporting and in-
13 vestigations, credit repair, credit clinics, or
14 check-cashing services.

15 (K) Laws that solely address facial rec-
16 ognition or facial recognition technologies, elec-
17 tronic surveillance, wiretapping, or telephone
18 monitoring.

19 (L) The Biometric Information Privacy
20 Act (740 ICLS 14 et seq.) and the Genetic In-
21 formation Privacy Act (410 ILCS 513 et seq.).

22 (M) Laws to address unsolicited email
23 messages, telephone solicitation, or caller ID.

1 (N) Laws that address health information,
2 medical information, medical records, HIV sta-
3 tus, or HIV testing.

4 (O) Laws that address the confidentiality
5 of library records.

6 (P) Section 1798.150 of the California
7 Civil Code (as amended on November 3, 2020
8 by initiative Proposition 24, Section 16).

9 (3) NONAPPLICATION OF FCC PRIVACY LAWS
10 AND REGULATIONS TO COVERED ENTITIES.—Not-
11 withstanding any other provision of law, Sections
12 222, 338(i), and 631 of the Communications Act of
13 1934, as amended, (47 U.S.C. §§ 222, 338(i), and
14 551) and any regulation promulgated by the Federal
15 Communications Commission under such sections,
16 shall not apply to any covered entity with respect to
17 the collecting, processing, or transferring of covered
18 data under this Act.

19 (c) PRESERVATION OF COMMON LAW OR STATUTORY
20 CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this
21 Act, nor any amendment, standard, rule, requirement, as-
22 sessment, law or regulation promulgated under this Act,
23 shall be construed to preempt, displace, or supplant any
24 Federal or State common law rights or remedies, or any
25 statute creating a remedy for civil relief, including any

1 cause of action for personal injury, wrongful death, prop-
2 erty damage, or other financial, physical, reputational, or
3 psychological injury based in negligence, strict liability,
4 products liability, failure to warn, an objectively offensive
5 intrusion into the private affairs or concerns of the indi-
6 vidual, or any other legal theory of liability under any Fed-
7 eral or State common law, or any State statutory law, ex-
8 cept that the fact of a violation of this Act shall not be
9 pleaded as an element of any such cause of action.

10 **SEC. 405. SEVERABILITY.**

11 If any provision of this Act, or the application thereof
12 to any person or circumstance, is held invalid, the remain-
13 der of this Act and the application of such provision to
14 other persons not similarly situated or to other cir-
15 cumstances shall not be affected by the invalidation.

16 **SEC. 406. COPPA.**

17 (a) IN GENERAL.—Nothing in this Act shall be con-
18 strued to relieve or change any obligations that a covered
19 entity or another person may have under the Children’s
20 Online Privacy Protection Act of 1998 (15 U.S.C. 6501
21 et seq.).

22 (b) UPDATED REGULATIONS.—Not later than 180
23 days after the enactment of this Act, the Commission shall
24 amend its rules issued pursuant to the Children’s Online
25 Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.)

1 to make reference to the additional requirements placed
2 on covered entities under this act, in addition to those al-
3 ready enacted under the Children’s Online Privacy Protec-
4 tion Act of 1998 that may already apply to some of such
5 covered entities.

6 **SEC. 407. AUTHORIZATION OF APPROPRIATIONS.**

7 There are authorized to be appropriated to the Com-
8 mission such sums as necessary to carry out this act.

9 **SEC. 408. EFFECTIVE DATE.**

10 Except as otherwise provided, this Act shall take ef-
11 fect on the date that is 180 days after the date of enact-
12 ment of this Act.

