

[DISCUSSION DRAFT]

118TH CONGRESS
2^D SESSION

H. R. _____

To [_____] , and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mrs. RODGERS of Washington introduced the following bill; which was referred to the Committee on _____

A BILL

To [_____] , and for other purposes.

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

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “American Privacy Rights Act of 2024”.

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

Sec. 1. Short title; table of contents.

TITLE I—AMERICAN PRIVACY RIGHTS

Sec. 101. Definitions.
Sec. 102. Data minimization.
Sec. 103. Privacy by design.
Sec. 104. Transparency.

1 a teen, an affirmative act by the parent or the
2 teen that—

3 (i) clearly communicates the author-
4 ization of the individual for an act or prac-
5 tice; and

6 (ii) is provided in response to a spe-
7 cific request from a covered entity, or a
8 service provider on behalf of a covered en-
9 tity, that meets the requirements of sub-
10 paragraph (B).

11 (B) REQUEST REQUIREMENTS.—The re-
12 quirements of this subparagraph with respect to
13 a request made under subparagraph (A) are the
14 following:

15 (i) The request is provided to the indi-
16 vidual in a clear and conspicuous stand-
17 alone disclosure.

18 (ii) The request includes a description
19 of each act or practice for which the con-
20 sent of the individual is sought and—

21 (I) clearly distinguishes between
22 an act or practice that is necessary,
23 proportionate, and limited to fulfill a
24 request of the individual and an act or
25 practice that is for another purpose;

1 (II) clearly states the specific
2 categories of covered data that the
3 covered entity shall collect, process,
4 retain, or transfer to fulfill the act or
5 practice for which the request was
6 made; and

7 (III) is written in easy-to-under-
8 stand language and includes a promi-
9 nent heading that would enable a rea-
10 sonable individual to identify and un-
11 derstand each such act or practice.

12 (iii) The request clearly explains the
13 applicable rights of the individual related
14 to consent.

15 (iv) The request is made in a manner
16 reasonably accessible to and usable by indi-
17 viduals living with disabilities.

18 (v) The request is made available to
19 the individual in the language in which the
20 covered entity provides a product or service
21 for which authorization is sought.

22 (vi) The option to refuse consent is at
23 least as prominent as the option to provide
24 consent, and the option to refuse consent
25 takes no more than 1 additional step as

1 compared to the number of steps necessary
2 to provide consent.

3 (vii) With respect to affirmative ex-
4 press consent sought for the collection,
5 processing, retention, or transfer of bio-
6 metric information or genetic information,
7 includes in the request for affirmative ex-
8 press consent the length of time the cov-
9 ered entity or service provider intends to
10 retain the biometric information or genetic
11 information, or, if it is not possible to iden-
12 tify the length of time, the criteria used to
13 determine the length of time the covered
14 entity or service provider intends to retain
15 the biometric information or genetic infor-
16 mation.

17 (C) EXPRESS CONSENT REQUIRED.—Af-
18 firmative express consent to an act or practice
19 may not be inferred from the inaction of an in-
20 dividual or the continued use by an individual
21 of a service or product provided by an entity.

22 (D) WITHDRAWAL OF AFFIRMATIVE EX-
23 PRESS CONSENT.—

24 (i) IN GENERAL.—A covered entity
25 shall provide an individual with a means to

1 withdraw affirmative express consent pre-
2 viously provided by the individual.

3 (ii) REQUIREMENTS.—The means to
4 withdraw affirmative express consent de-
5 scribed in clause (i) shall be—

6 (I) clear and conspicuous; and

7 (II) as easy for a reasonable indi-
8 vidual to use as the mechanism by
9 which the individual provided affirma-
10 tive express consent.

11 (2) BIOMETRIC INFORMATION.—

12 (A) IN GENERAL.—The term “biometric
13 information” means any covered data that al-
14 lows or confirms the unique identification or
15 verification of an individual and is generated
16 from the measurement or processing of unique
17 biological, physical, or physiological characteris-
18 tics, including—

19 (i) fingerprints;

20 (ii) voice prints;

21 (iii) iris or retina imagery scans;

22 (iv) facial or hand mapping, geometry,
23 or templates; and

24 (v) gait.

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

- 3 (i) a digital or physical photograph;
4 (ii) an audio or video recording; or
5 (iii) data derived from a digital or
6 physical photograph or an audio or video
7 recording that cannot be used to identify
8 or authenticate a specific individual.

9 (3) CHILD.—The term “child” means an indi-
10 vidual under the age of 13.

11 (4) CLEAR AND CONSPICUOUS.—The term
12 “clear and conspicuous” means, with respect to a
13 disclosure, that the disclosure is difficult to miss and
14 easily understandable by ordinary consumers.

15 (5) COARSE GEOLOCATION INFORMATION.—The
16 term “coarse geolocation information” means infor-
17 mation that reveals the present physical location of
18 an individual or device identified by a unique per-
19 sistent identifier at the ZIP code attribution level,
20 except where a geographic area attributed to a ZIP
21 code is equal to or less than the area of a circle with
22 a radius of 1,850 feet or less, at a level greater than
23 a geographic area equal to the area of a circle with
24 a radius of 1,850 feet.

1 (6) COLLECT; COLLECTION.—The terms “col-
2 lect” and “collection” mean, with respect to covered
3 data, buying, renting, gathering, obtaining, receiv-
4 ing, accessing, or otherwise acquiring the covered
5 data by any means.

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

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

11 (9) CONNECTED DEVICE.—The term “con-
12 nected device” means a device that is capable of con-
13 necting to the internet.

14 (10) CONTEXTUAL ADVERTISING.—The term
15 “contextual advertising” means displaying or pre-
16 senting an advertisement that—

17 (A) does not vary based on the identity of
18 the individual recipient; and

19 (B) is based solely on—

20 (i) the content of a webpage or online
21 service;

22 (ii) a specific request of the individual
23 for information or feedback; or

24 (iii) coarse geolocation information.

1 (11) CONTROL.—The term “control” means,
2 with respect to an entity—

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

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

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

11 (12) COVERED DATA.—

12 (A) IN GENERAL.—The term “covered
13 data” means information that identifies or is
14 linked or reasonably linkable, alone or in com-
15 bination with other information, to an indi-
16 vidual or a device that identifies or is linked or
17 reasonably linkable to 1 or more individuals.

18 (B) EXCLUSIONS.—The term “covered
19 data” does not include—

20 (i) de-identified data;

21 (ii) employee information;

22 (iii) publicly available information;

23 (iv) inferences made exclusively from
24 multiple independent sources of publicly
25 available information, if such inferences—

1 (I) do not reveal information
2 about an individual that meets the
3 definition of the term “sensitive cov-
4 ered data” with respect to the indi-
5 vidual; and

6 (II) are not combined with cov-
7 ered data;

8 (v) information in the collection of a
9 library, archive, or museum, if—

10 (I) the collection is—

11 (aa) open to the public or
12 routinely made available to re-
13 searchers who are not affiliated
14 with the library, archive, or mu-
15 seum; and

16 (bb) composed of lawfully
17 acquired materials with respect
18 to which all licensing conditions
19 are met; and

20 (II) the library, archive, or mu-
21 seum has—

22 (aa) a public service mission;
23 and

24 (bb) trained staff or volun-
25 teers to provide professional serv-

1 ices normally associated with li-
2 braries, archives, or museums; or
3 (vi) on-device data.

4 (13) COVERED ENTITY.—

5 (A) IN GENERAL.—The term “covered en-
6 tity” means any entity that, alone or jointly
7 with others, determines the purposes and means
8 of collecting, processing, retaining, or transfer-
9 ring covered data and—

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

12 (ii) is a common carrier subject to
13 title II of the Communications Act of 1934
14 (47 U.S.C. 201 et seq.); or

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

18 (B) INCLUSION.—The term “covered enti-
19 ty” includes any entity that controls, is con-
20 trolled by, or is under common control with an-
21 other covered entity.

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

24 (i) a Federal, State, Tribal, or local
25 government entity, such as a body, author-

1 ity, board, bureau, commission, district,
2 agency, or other political subdivision of the
3 Federal Government or a State, Tribal, or
4 local government;

5 (ii) an entity that is collecting, proc-
6 essing, retaining, or transferring covered
7 data on behalf of a Federal, State, Tribal,
8 or local government entity, to the extent
9 that such entity is acting as a service pro-
10 vider to the government entity;

11 (iii) a small business;

12 (iv) an individual acting at their own
13 direction and in a non-commercial context;

14 (v) the National Center for Missing
15 and Exploited Children; or

16 (vi) except with respect to require-
17 ments under section 109, a nonprofit orga-
18 nization whose primary mission is to pre-
19 vent, investigate, or deter fraud, to train
20 anti-fraud professionals, or to educate the
21 public about fraud, including insurance
22 fraud, securities fraud, and financial fraud,
23 to the extent the organization collects,
24 processes, retains, or transfers covered

1 data in furtherance of such primary mis-
2 sion.

3 (D) NONAPPLICATION TO SERVICE PRO-
4 VIDERS.—An entity may not be considered to
5 be a “covered entity” for the purposes of this
6 title, insofar as the entity is acting as a service
7 provider.

8 (14) COVERED HIGH-IMPACT SOCIAL MEDIA
9 COMPANY.—

10 (A) IN GENERAL.—The term “covered
11 high-impact social media company” means a
12 covered entity that provides any internet-acces-
13 sible platform that—

14 (i) generates \$3,000,000,000 or more
15 in global annual revenue, including the rev-
16 enue generated by any affiliate of such cov-
17 ered entity;

18 (ii) has 300,000,000 or more global
19 monthly active users for not fewer than 3
20 of the preceding 12 months; and

21 (iii) constitutes an online product or
22 service that is primarily used by users to
23 access or share user-generated content.

24 (B) TREATMENT OF CERTAIN SERVICES
25 AND APPLICATIONS.—A service or application

1 may not be considered to constitute an online
2 product or service described in subparagraph
3 (A)(iii) solely on the basis of providing any of
4 the following:

5 (i) Email.

6 (ii) Career or professional develop-
7 ment networking opportunities.

8 (iii) Reviews of products, services,
9 events, or destinations.

10 (iv) A platform for use in a public or
11 private school under the direction of the
12 school.

13 (v) File collaboration.

14 (vi) Cloud storage.

15 (vii) Closed video or audio commu-
16 nications services.

17 (viii) A wireless messaging service, in-
18 cluding such a service provided through
19 short messaging service or multimedia
20 messaging service protocols, that is not a
21 component of, or linked to, a platform of
22 a covered high-impact social media com-
23 pany, if the predominant or exclusive func-
24 tion is direct messaging consisting of the
25 transmission of text, photos, or videos that

1 are sent by electronic means, and if mes-
2 sages are transmitted from the sender to a
3 recipient and are not posted within a plat-
4 form of a covered high-impact social media
5 company or publicly.

6 (15) COVERED MINOR.—The term “covered
7 minor” means an individual under the age of 17.

8 (16) DARK PATTERNS.—The term “dark pat-
9 terns” means a user interface designed or manipu-
10 lated with the substantial effect of subverting or im-
11 pairing user autonomy, decision-making, or choice.

12 (17) DATA BROKER.—

13 (A) IN GENERAL.—The term “data
14 broker” means a covered entity whose principal
15 source of revenue is derived from processing or
16 transferring covered data that the covered enti-
17 ty did not collect directly from the individuals
18 linked or linkable to the covered data.

19 (B) PRINCIPAL SOURCE OF REVENUE.—

20 For purposes of this paragraph, the term “prin-
21 cipal source of revenue” means, for the prior
22 12-month period—

23 (i) revenue that constitutes greater
24 than 50 percent of all revenue of the cov-
25 ered entity during such period; or

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

7 (C) NON-APPLICATION TO SERVICE PRO-
8 VIDERS.—The term “data broker” does not in-
9 clude an entity to the extent that such entity is
10 acting as a service provider.

11 (18) DE-IDENTIFIED DATA.—

12 (A) IN GENERAL.—The term “de-identified
13 data” means information that cannot reason-
14 ably be used to infer or derive the identity of
15 an individual, and does not identify and is not
16 linked or reasonably linkable to an individual or
17 a device that identifies or is linked or reason-
18 ably linkable to an individual, regardless of
19 whether the information is aggregated, if the
20 relevant covered entity or service provider—

21 (i) takes reasonable physical, adminis-
22 trative, and technical measures to ensure
23 that the information cannot, at any point,
24 be used to re-identify any individual or de-

1 vice that identifies or is linked or reason-
2 ably linkable to an individual;

3 (ii) publicly commits in a clear and
4 conspicuous manner to—

5 (I) process, retain, or transfer
6 the information solely in a de-identi-
7 fied form without any reasonable
8 means for re-identification; and

9 (II) not attempt to re-identify the
10 information with any individual or de-
11 vice that identifies or is linked or rea-
12 sonably linkable to an individual, ex-
13 cept as necessary, limited, and propor-
14 tionate to test the effectiveness of the
15 measures described in clause (i); and

16 (iii) contractually obligates any entity
17 that receives the information from the cov-
18 ered entity or service provider to—

19 (I) comply with clauses (i) and
20 (ii) with respect to the information;
21 and

22 (II) require that such contractual
23 obligations be included contractually
24 in all subsequent instances in which
25 the information may be received.

1 (B) HEALTH INFORMATION.—The term
2 “de-identified data” includes health information
3 (as defined in section 1171 of the Social Secu-
4 rity Act (42 U.S.C. 1320d)) that has been de-
5 identified in accordance with section 164.514(b)
6 of title 45, Code of Federal Regulations, except
7 that if such information is subsequently pro-
8 vided to an entity that is not an entity subject
9 to parts 160 and 164 of such title 45, such en-
10 tity shall comply with clauses (ii) and (iii) of
11 subparagraph (A) for the information to be con-
12 sidered de-identified under this title.

13 (19) DERIVED DATA.—The term “derived data”
14 means covered data that is created by the derivation
15 of information, data, assumptions, correlations, in-
16 ferences, predictions, or conclusions from facts, evi-
17 dence, or another source of information.

18 (20) DEVICE.—The term “device” means any
19 electronic equipment capable of collecting, proc-
20 essing, retaining, or transferring covered data that is
21 used by 1 or more individuals, including a connected
22 device or a portable connected device.

23 (21) DIRECT MAIL TARGETED ADVERTISING.—
24 The term “direct mail targeted advertising” means
25 advertising or marketing using third-party data

1 through a direct communication with an individual
2 via direct mail.

3 (22) DISABILITY.—The term “disability” has
4 the meaning given to such term in the Americans
5 with Disabilities Act (42 U.S.C. 12102).

6 (23) EMAIL TARGETED ADVERTISING.—The
7 term “email targeted advertising” means advertising
8 or marketing using third-party data through a direct
9 communication with an individual via email.

10 (24) EMPLOYEE.—The term “employee” means
11 an individual who is an employee, director, officer,
12 staff member, paid intern, individual working as an
13 independent contractor (who is not a service pro-
14 vider), volunteer, or unpaid intern of an employer,
15 regardless of whether such individual is paid, un-
16 paid, or engaged on a temporary basis.

17 (25) EMPLOYEE INFORMATION.—The term
18 “employee information” means information, includ-
19 ing biometric information or genetic information—

20 (A) about an individual in the course of
21 employment or application for employment (in-
22 cluding on a contract or temporary basis), if
23 such information is collected, retained, proc-
24 essed, or transferred by the employer or the
25 service provider of the employer solely for pur-

1 poses necessary for the employment or applica-
2 tion of the individual;

3 (B) that is emergency contact information
4 for an individual who is an employee or job ap-
5 plicant of the employer, if such information is
6 collected, retained, processed, or transferred by
7 the employer or the service provider of the em-
8 ployer solely for the purpose of having an emer-
9 gency contact for such individual on file; or

10 (C) about an individual who is an employee
11 or former employee of the employer, or the rel-
12 ative, dependent or beneficiary of the employee
13 or former employee, for the purpose of admin-
14 istering benefits, including enrollment and
15 disenrollment for benefits, to which such indi-
16 vidual, relative, dependent, or beneficiary is en-
17 titled on the basis of the employment of the in-
18 dividual with the employer, if such information
19 is collected, retained, processed, or transferred
20 by the employer or the service provider of the
21 employer solely for the purpose of administering
22 such benefits.

23 (26) ENTITY.—The term “entity” means an in-
24 dividual, a trust, a partnership, an association, an
25 organization, a company, and a corporation.

1 (27) EXECUTIVE AGENCY.—The term “Execu-
2 tive agency” has the meaning given such term in
3 section 105 of title 5, United States Code.

4 (28) FEDERATED NONPROFIT ORGANIZA-
5 TION.—The term “federated nonprofit organization”
6 means a network or system of 2 or more entities, de-
7 scribed in section 501(c)(3) of the Internal Revenue
8 Code of 1986 and exempt from taxation under sec-
9 tion 501(a) of such Code, that share common brand-
10 ing.

11 (29) FIRST PARTY.—The term “first party”
12 means a consumer-facing covered entity with which
13 the consumer intends and expects to interact, and
14 includes any entities with which the covered entity
15 shares common branding.

16 (30) FIRST-PARTY ADVERTISING.—

17 (A) IN GENERAL.—The term “first-party
18 advertising” means advertising or marketing by
19 a first party using that first party’s first-party
20 data and not other forms of covered data—

21 (i) through direct communications
22 with an individual, such as direct mail,
23 email (subject to 15 U.S.C. 103 and all
24 regulations promulgated thereunder), or
25 text message communications (subject to

1 47 U.S.C. 227 and all regulations promul-
2 gated thereunder); or

3 (ii) entirely within the following first
4 party contexts—

5 (I) in a physical location oper-
6 ated by the first party;

7 (II) on a website, online service,
8 online application, or mobile applica-
9 tion operated by a first party (other
10 than a covered high-impact social
11 media company) to display or present
12 an online advertisement that promotes
13 a product or service (whether offered
14 by the first party or not offered by
15 the first party) to an individual or de-
16 vice identified by a unique persistent
17 identifier, or group of individuals or
18 devices identified by unique persistent
19 identifiers; or

20 (III) on a website, online service,
21 online application, or mobile applica-
22 tion operated by a first party that is
23 a covered high-impact social media
24 company to display or present an on-
25 line advertisement that promotes a

1 product or service offered by the first
2 party that is a covered high-impact
3 social media company to an individual
4 or device identified by a unique per-
5 sistent identifier, or group of individ-
6 uals or devices identified by unique
7 persistent identifiers.

8 (B) EXCLUSION.—The term “first-party
9 advertising” does not include contextual adver-
10 tising.

11 (31) FIRST-PARTY DATA.—The term “first-
12 party data” means covered data collected directly
13 from an individual by a first party, including based
14 on a visit by the individual to or use by the indi-
15 vidual of a physical location, a website, online serv-
16 ice, online application, or mobile application oper-
17 ated by the first party.

18 (32) GENETIC INFORMATION.—The term “ge-
19 netic information” means any covered data, regard-
20 less of format, that concerns the genetic characteris-
21 tics of an identified or identifiable individual, includ-
22 ing—

23 (A) raw sequence data that results from
24 the sequencing of the complete, or a portion of,

1 extracted deoxyribonucleic acid (DNA) of an in-
2 dividual; or

3 (B) genotypic and phenotypic information
4 that results from analyzing raw sequence data
5 described in subparagraph (A).

6 (33) HEALTH INFORMATION.—The term
7 “health information” means information that de-
8 scribes or reveals the past, present, or future phys-
9 ical health, mental health, disability, diagnosis, or
10 health condition health status, or treatment of an in-
11 dividual, including the precise geolocation informa-
12 tion of such treatment.

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

16 (35) KNOWLEDGE.—

17 (A) IN GENERAL.—The term “knowledge”
18 with respect to knowledge that an individual is
19 a child, teen, or covered minor means actual
20 knowledge or knowledge fairly implied on the
21 basis of objective circumstances.

22 (B) RULE OF CONSTRUCTION.—For pur-
23 poses of enforcing this title or a regulation pro-
24 mulgated under this title, a determination as to
25 whether a covered entity has knowledge fairly

1 implied on the basis of objective circumstances
2 that a individual is a child or teen shall rely on
3 competent and reliable evidence, taking into ac-
4 count the totality of the circumstances, includ-
5 ing whether a reasonable and prudent person
6 under the circumstances would have known that
7 the individual is a child or teen. Nothing in this
8 title, including a determination described in the
9 preceding sentence, shall be construed to re-
10 quire a covered entity to—

11 (i) affirmatively collect any covered
12 data with respect to the age of a child or
13 teen that an covered entity is not already
14 collecting in the normal course of business;
15 or

16 (ii) implement an age gating or age
17 verification functionality.

18 (C) COMMISSION GUIDANCE.—

19 (i) IN GENERAL.—Within 180 days of
20 enactment, the Commission shall issue
21 guidance to provide information, including
22 best practices and examples for covered en-
23 tities to understand the Commission’s de-
24 termination of whether a covered entity
25 has knowledge fairly implied on the basis

1 of objective circumstances that an indi-
2 vidual is a child or teen.

3 (ii) LIMITATION.—No guidance issued
4 by the Commission with respect to this
5 title shall confer any rights on any person,
6 State, or locality, nor shall operate to bind
7 the Commission or any person to the ap-
8 proach recommended in such guidance.
9 Any enforcement action brought pursuant
10 to this title, by the Commission or State
11 attorney general, as applicable, shall allege
12 a specific violation of a provision of this
13 title and may not base an enforcement ac-
14 tion on, or as applicable execute a consent
15 order based on, practices that are alleged
16 to be inconsistent with any such guidance,
17 unless the practices allegedly violate this
18 title.

19 (36) LARGE DATA HOLDER.—

20 (A) IN GENERAL.—The term “large data
21 holder” means a covered entity or service pro-
22 vider that, in the most recent calendar year,
23 had an annual gross revenue of not less than
24 \$250,000,000 and, subject to subparagraph

1 (B), collected, processed, retained, or trans-
2 ferred—

3 (i) the covered data of—

4 (I) more than 5,000,000 individ-
5 uals;

6 (II) more than 15,000,000 port-
7 able connected devices that identify or
8 are linked or reasonably linkable to 1
9 or more individuals; or

10 (III) more than 35,000,000 con-
11 nected devices that identify or are
12 linked or reasonable linkable to 1 or
13 more individuals; or

14 (ii) the sensitive covered data of—

15 (I) more than 200,000 individ-
16 uals;

17 (II) more than 300,000 portable
18 connected devices that identify or are
19 linked or reasonable linkable to 1 or
20 more individuals; or

21 (III) more than 700,000 con-
22 nected devices that identify or are
23 linked or reasonably linkable to 1 or
24 more individuals.

1 (B) EXCLUSIONS.—For the purposes of
2 subparagraph (A), a covered entity or service
3 provider may not be considered a large data
4 holder solely on the basis of collecting, proc-
5 essing, retaining, or transferring to a service
6 provider—

7 (i) personal mailing or email address-
8 es;

9 (ii) personal telephone numbers;

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

14 (iv) in the case of a covered entity
15 that is a seller of goods or services (other
16 than an entity that facilitates payment,
17 such as a bank, credit card processor, mo-
18 bile payment system, or payment plat-
19 form), credit, debit, or mobile payment in-
20 formation necessary and used to initiate,
21 render, bill for, finalize, complete, or other-
22 wise facilitate payments for such goods or
23 services.

24 (C) DEFINITION OF ANNUAL GROSS REV-
25 ENUE.—For the purposes of subparagraph (A),

1 the term “annual gross revenue”, with respect
2 to a covered entity or service provider—

3 (i) means the gross receipts the cov-
4 ered entity or service provider received, in
5 whatever form from all sources, without
6 subtracting any costs or expenses; and

7 (ii) includes contributions, gifts,
8 grants, dues or other assessments, income
9 from investments, and proceeds from the
10 sale of real or personal property.

11 (37) MARKET RESEARCH.—The term “market
12 research” means the collection, processing, retention,
13 or transfer of covered data, with affirmative express
14 consent, that is necessary, proportionate, and limited
15 to measure and analyze the market or market trends
16 of products, services, advertising, or ideas, if the
17 covered data is not—

18 (A) integrated into any product or service;

19 (B) otherwise used to contact any indi-
20 vidual or device of an individual; or

21 (C) used for targeted advertising or to oth-
22 erwise market to any individual or device of an
23 individual.

24 (38) MATERIAL CHANGE.—The term “material
25 change” means, with respect to treatment of covered

1 data, a change by an entity that would likely affect
2 the decision of an individual to engage with and pro-
3 vide covered data to the entity, including providing
4 affirmative express consent for, or opt out of, the
5 collection, processing, retention, or transfer of cov-
6 ered data pertaining to such individual.

7 (39) MOBILE APPLICATION.—The term “mobile
8 application”—

9 (A) means a software program that runs
10 on the operating system of—

11 (i) a cellular telephone;

12 (ii) a tablet computer; or

13 (iii) a similar portable computing de-
14 vice that transmits data over a wireless
15 connection; and

16 (B) includes a service or application of-
17 fered via a connected device.

18 (40) ON-DEVICE DATA.—

19 (A) IN GENERAL.—The term “on-device
20 data” means data collected, retained, and proc-
21 essed solely on an individual’s device.

22 (B) LIMITATION.—Data collected, re-
23 tained, and processed solely on an individual’s
24 device shall be considered “on-device data” only
25 if—

1 (i) such data is not transferred by a
2 covered entity or service provider;

3 (ii) the covered entity clearly and con-
4 spicuously provides the device owner with
5 controls that allow the owner to access,
6 correct, delete, and export such data con-
7 sistent with the rights provided with re-
8 spect to covered data pursuant to section
9 105;

10 (iii) the covered entity provides easy
11 to understand instructions on how the de-
12 vice owner can access such controls; and

13 (iv) the covered entity establishes, im-
14 plements, and maintains reasonable data
15 security practices, consistent with section
16 109, to protect—

17 (I) the confidentiality, integrity,
18 and availability of the on-device data;
19 and

20 (II) on device data against unau-
21 thorized access.

22 (41) ONLINE ACTIVITY PROFILE.—The term
23 “online activity profile” means covered data that
24 identifies the online activities of an individual (or a
25 device linked or reasonably linkable to an individual)

1 over time and across third party websites, online
2 services, online applications, or mobile applications
3 that do not share common branding, that is col-
4 lected, processed, retained, or transferred for the
5 purpose of evaluating, analyzing, or predicting the
6 behaviors or characteristics of an individual.

7 (42) ONLINE APPLICATION.—The term “online
8 application”—

9 (A) means an internet-connected software
10 program; and

11 (B) includes a service or application of-
12 fered via a connected device.

13 (43) PARENT.—The term “parent” means a
14 legal guardian.

15 (44) PORTABLE CONNECTED DEVICE.—The
16 term “portable connected device” means a portable
17 device that is capable of connecting to the internet
18 over a wireless connection, including a smartphone,
19 tablet computer, laptop computer, smartwatch, or
20 similar portable device.

21 (45) PRECISE GEOLOCATION INFORMATION.—

22 (A) IN GENERAL.—The term “precise
23 geolocation information” means information
24 that reveals the past or present physical loca-
25 tion of an individual or device with sufficient

1 precision to identify the location of such indi-
2 vidual or device within a geographic area that
3 is equal to or less than the area of a circle with
4 a radius of 1,850 feet or less.

5 (B) EXCLUSIONS.—The term “precise
6 geolocation information” does not include infor-
7 mation derived solely from—

- 8 (i) a digital or physical photograph;
9 (ii) an audio or visual recording; or
10 (iii) metadata associated with a digital
11 or physical photograph or an audio record-
12 ing that cannot be linked to an individual.

13 (46) PROCESS.—The term “process” means,
14 with respect to covered data, any operation or set of
15 operations performed on the covered data, including
16 analyzing, organizing, structuring, using, modifying,
17 or otherwise handling the covered data.

18 (47) PUBLICLY AVAILABLE INFORMATION.—

19 (A) IN GENERAL.—The term “publicly
20 available information” means any information
21 that a covered entity has a reasonable basis to
22 believe has been lawfully made available to the
23 general public by—

- 24 (i) Federal, State, or local government
25 records, if the covered entity collects, proc-

1 esses, retains, and transfers such informa-
2 tion in accordance with any restrictions or
3 terms of use placed on the information by
4 the relevant government entity;

5 (ii) widely distributed media;

6 (iii) a website or online service made
7 available to all members of the public, for
8 free or for a fee, including where all mem-
9 bers of the public can log in to the website
10 or online service; or

11 (iv) a disclosure to the general public
12 that is required to be made by Federal,
13 State, or local law.

14 (B) CLARIFICATIONS; LIMITATIONS.—

15 (i) AVAILABLE TO ALL MEMBERS OF
16 THE PUBLIC.—For purposes of this para-
17 graph, information from a website or on-
18 line service is not available to all members
19 of the public if the individual to whom the
20 information pertains has restricted the in-
21 formation to a specific audience or main-
22 tained a default setting that restricts the
23 information to a specific audience.

24 (ii) BUSINESS CONTACT INFORMA-
25 TION.—The term “publicly available infor-

1 mation” includes business contact informa-
2 tion of an individual acting in a business
3 or professional context that is made avail-
4 able on a website or online service made
5 available to all members of the public, in-
6 cluding the individual’s name, position or
7 title, business telephone number, business
8 email address, or business address of the
9 employee.

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

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

16 (II) derived data from publicly
17 available information that reveals in-
18 formation about an individual that
19 meets the definition of the term “sen-
20 sitive covered data”;

21 (III) biometric information;

22 (IV) genetic information, unless
23 made publicly available by the indi-
24 vidual to whom the information per-

1 tains by a means described in clause
2 (ii) or (iii) of subparagraph (A);

3 (V) covered data that is created
4 through the combination of covered
5 data with publicly available informa-
6 tion;

7 (VI) intimate images, authentic
8 or computer-generated, known to be
9 nonconsensual; or

10 (VII) sensitive covered data made
11 available by a data broker.

12 (48) RETAIN.—The term “retain” means, with
13 respect to covered data, to store, maintain, save, or
14 otherwise keep such data, regardless of format.

15 (49) SENSITIVE COVERED DATA.—

16 (A) IN GENERAL.—The term “sensitive
17 covered data” means the following forms of cov-
18 ered data:

19 (i) A government-issued identifier, in-
20 cluding a Social Security number, passport
21 number, or driver’s license number, that is
22 not required by law to be displayed in pub-
23 lic.

24 (ii) Any information that describes or
25 reveals the past, present, or future physical

1 health, mental health, disability, diagnosis,
2 health condition or health status, treat-
3 ment of an individual.

4 (iii) Genetic information.

5 (iv) A financial account number, debit
6 card number, credit card number, or any
7 required security or access code, password,
8 or credentials allowing access to any such
9 account or card, except that the last four
10 digits of an account number, debit card
11 number, or credit card number may not be
12 considered sensitive covered data.

13 (v) Biometric information.

14 (vi) Precise geolocation information.

15 (vii) The private communications of
16 an individual (such as voicemails, or other
17 voice or video communications, emails,
18 texts, direct messages, or mail) or informa-
19 tion identifying the parties to such commu-
20 nications, information contained in tele-
21 phone bills, and any information that per-
22 tains to the transmission of private voice
23 or video communications, including num-
24 bers called, numbers from which calls were
25 placed, the time calls were made, call dura-

1 tion, and location information of the par-
2 ties to the call, unless the covered entity or
3 service provider is an intended recipient of
4 the communication.

5 (viii) Unencrypted or unredacted ac-
6 count or device log-in credentials.

7 (ix) Information revealing the sexual
8 behavior of an individual in a manner in-
9 consistent with the reasonable expectation
10 of the individual regarding disclosure of
11 such information.

12 (x) Calendar information, address
13 book information, phone, text, or electronic
14 logs, photographs, audio recordings, or vid-
15 eos intended for private use.

16 (xi) A photograph, film, video record-
17 ing, or other similar medium that shows
18 the naked or undergarment-clad private
19 area of an individual.

20 (xii) Information revealing the extent
21 or content of the access, viewing, or other
22 use by an individual of any video program-
23 ming (as defined in section 713(h)(2) of
24 the Communications Act of 1934 (47
25 U.S.C. 613(h)(2))), including program-

1 ming provided by a provider of broadcast
2 television service, cable service, satellite
3 service, or streaming media service, but
4 only with regard to the transfer of such in-
5 formation to a third party (excluding any
6 such information used solely for transfers
7 for independent video measurement).

8 (xiii) Information collected by a cov-
9 ered entity that is not a provider of a serv-
10 ice described in clause (xii) that reveals the
11 video content requested or selected by an
12 individual (excluding any such information
13 used solely for transfers for independent
14 video measurement).

15 (xiv) Information revealing the race,
16 ethnicity, national origin, religion, or sex of
17 an individual in a manner inconsistent
18 with the reasonable expectation of the indi-
19 vidual regarding disclosure of such infor-
20 mation.

21 (xv) An online activity profile.

22 (xvi) Information about a covered
23 minor.

1 (xvii) Information that reveals the sta-
2 tus of an individual as a member of the
3 Armed Forces.

4 (xviii) Neural data.

5 (xix) Any other covered data collected,
6 processed, retained, or transferred for the
7 purpose of identifying the types of infor-
8 mation described in clauses (i) through
9 (xviii).

10 (B) THIRD PARTY.—For the purposes of
11 subparagraph (A)(xii), the term “third party”
12 does not include an entity that—

13 (i) is related by common ownership or
14 corporate control to the provider of broad-
15 cast television service or streaming media
16 service; and

17 (ii) provides video programming as de-
18 scribed in such subparagraph.

19 (50) SERVICE PROVIDER.—

20 (A) IN GENERAL.—The term “service pro-
21 vider” means an entity that collects, processes,
22 retains, or transfers covered data for the pur-
23 pose of performing 1 or more services or func-
24 tions on behalf of, and at the direction of—

1 (i) a covered entity or another service
2 provider; or

3 (ii) a Federal, State, Tribal, terri-
4 torial, or local government entity.

5 (B) RULE OF CONSTRUCTION.—

6 (i) IN GENERAL.—An entity is a cov-
7 ered entity and not a service provider with
8 respect to a specific collecting, processing,
9 retaining, or transferring of covered data,
10 if the entity, jointly or with others, deter-
11 mines the purposes and means of the spe-
12 cific collecting, processing, retaining, or
13 transferring of data.

14 (ii) INSTRUCTIONS.—A person that is
15 not limited in its collecting, processing, re-
16 tention, or transferring of covered data
17 pursuant to the instructions of a covered
18 entity, another service provider, or a Fed-
19 eral, State, Tribal, territorial, or local gov-
20 ernment entity, or that fails to adhere to
21 such instructions, is a covered entity and
22 not a service provider with respect to a
23 specific processing of such data. If a serv-
24 ice provider begins, alone, or jointly with
25 others determining the purposes and

1 means of collecting, processing, retaining,
2 or transferring covered data, it is a covered
3 entity with respect to such data. A service
4 provider that continues to adhere to the in-
5 structions of a covered entity with respect
6 to processing covered data remains a serv-
7 ice provider.

8 (iii) CONTEXT REQUIRED.—Whether
9 an entity is a covered entity or a service
10 provider depends on the facts surrounding,
11 and the context in which, data is collected,
12 processed, retained, or transferred.

13 (51) SMALL BUSINESS.—

14 (A) IN GENERAL.—The term “small busi-
15 ness” means an entity (including any affiliate
16 of the entity)—

17 (i) that has average annual gross rev-
18 enues for the period of the 3 preceding cal-
19 endar years (or for the period during
20 which the entity has been in existence, if
21 such period is less than 3 calendar
22 years)not exceeding 40,000,000 million
23 dollars, indexed to the Producer Price
24 Index reported by the Bureau of Labor
25 Statistics;

1 (ii) that, on average for the period de-
2 scribed in clause (i), did not annually col-
3 lect, process, retain, or transfer the cov-
4 ered data of more than 200,000 individuals
5 for any purpose other than initiating, ren-
6 dering, billing for, finalizing, completing,
7 or otherwise collecting payment for a re-
8 quested service or product; and

9 (iii) that did not, during the period
10 described in clause (i), transfer covered
11 data to a third party in exchange for rev-
12 enue or anything of value, except for pur-
13 poses of initiating, rendering, billing for, fi-
14 nalizing, completing, or otherwise collecting
15 payment for a requested service or product
16 or facilitating web analytics that are not
17 used to create an online activity profile.

18 (B) NONPROFIT REVENUE.—For purposes
19 of subparagraph (A)(i), the term “revenue”, as
20 such term relates to any entity that is not orga-
21 nized to carry on business for its own profit or
22 that of its members, means the gross receipts
23 the entity received, in whatever form from all
24 sources, without subtracting any costs or ex-
25 penses, and includes contributions, gifts, grants

1 (except for grants from the Federal Govern-
2 ment), dues or other assessments, income from
3 investments, or proceeds from the sale of real
4 or personal property.

5 (52) STATE.—The term “State” means each of
6 the 50 States, the District of Columbia, the Com-
7 monwealth of Puerto Rico, the Virgin Islands of the
8 United States, Guam, American Samoa, and the
9 Commonwealth of the Northern Mariana Islands.

10 (53) SUBSTANTIAL PRIVACY HARM.—The term
11 “substantial privacy harm” means—

12 (A) any alleged financial harm of not less
13 than \$10,000; or

14 (B) any alleged physical or mental harm to
15 an individual that involves—

16 (i) treatment by a licensed,
17 credentialed, or otherwise bona fide health
18 care provider, hospital, community health
19 center, clinic, hospice, or residential or out-
20 patient facility for medical, mental health,
21 or addiction care; or

22 (ii) physical injury, highly offensive
23 intrusion into the privacy expectations of a
24 reasonable individual under the cir-
25 cumstances, or discrimination on the basis

1 of race, color, religion, national origin, sex,
2 or disability.

3 (54) TARGETED ADVERTISING.—The term “tar-
4 geted advertising”—

5 (A) means displaying or presenting an on-
6 line advertisement to an individual or to a de-
7 vice identified by a unique persistent identifier
8 (or to a group of individuals or devices identi-
9 fied by unique persistent identifiers), if the ad-
10 vertisement is selected based, in whole or in
11 part, on known or predicted preferences, or in-
12 terests associated with the individual or a de-
13 vice identified by a unique persistent identifier;

14 (B) includes—

15 (i) an online advertisement for a prod-
16 uct or service by a covered high-impact so-
17 cial media company that is not a product
18 or service offered by the covered high-im-
19 pact social media company; and

20 (ii) an online advertisement for a
21 product or service based on the previous
22 interaction of an individual or a device
23 identified by a unique persistent identifier
24 with such product or service on a website
25 or online service that does not share com-

1 mon branding or affiliation with the
2 website or online service displaying or pre-
3 senting the advertisement; and

4 (C) excludes contextual advertising and
5 first-party advertising.

6 (55) TEEN.—The term “teen” means an indi-
7 vidual over the age of 12 and under the age of 17.

8 (56) THIRD PARTY.—The term “third party”—

9 (A) means any entity that—

10 (i) receives covered data from another
11 entity that is not the individual to whom
12 the data pertains; and

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

15 (B) does not include an entity that collects
16 covered data from another entity if the 2 enti-
17 ties are—

18 (i) related by common ownership or
19 corporate control; or

20 (ii) nonprofit entities that are part of
21 the same federated nonprofit organization.

22 (57) THIRD-PARTY DATA.—The term “third-
23 party data” means covered data that has been trans-
24 ferred to a third party.

1 (58) TRANSFER.—The term “transfer” means,
2 with respect to covered data, to disclose, release,
3 share, disseminate, make available, sell, rent, or li-
4 cense the covered data (orally, in writing, electroni-
5 cally, or by any other means) for consideration of
6 any kind or for a commercial purpose.

7 (59) UNIQUE PERSISTENT IDENTIFIER.—

8 (A) IN GENERAL.—The term “unique per-
9 sistent identifier” means a technologically cre-
10 ated identifier to the extent that such identifier
11 is reasonably linkable to an individual or a de-
12 vice that identifies or is linked or reasonably
13 linkable to 1 or more individuals, including de-
14 vice identifiers, Internet Protocol addresses,
15 cookies, beacons, pixel tags, mobile ad identi-
16 fiers or similar technology customer numbers,
17 unique pseudonyms, user aliases, telephone
18 numbers, or other forms of persistent or prob-
19 abilistic identifiers that are linked or reasonably
20 linkable to 1 or more individuals or devices.

21 (B) EXCLUSION.—The term “unique per-
22 sistent identifier” does not include an identifier
23 assigned by a covered entity for the sole pur-
24 pose of giving effect to the exercise of affirma-
25 tive express consent by an individual or opt out

1 by an individual with respect to the collecting,
2 processing, retaining, and transfer of covered
3 data or otherwise limiting the collecting, proc-
4 essing, retaining, or transfer of such covered
5 data.

6 (60) WIDELY DISTRIBUTED MEDIA.—

7 (A) IN GENERAL.—The term “widely dis-
8 tributed media” means information that is
9 available to the general public, including infor-
10 mation from a telephone book or online direc-
11 tory, a television, internet, or radio program,
12 the news media, or an internet site that is avail-
13 able to the general public on an unrestricted
14 basis.

15 (B) EXCLUSION.—The term “widely dis-
16 tributed media” does not include an obscene
17 visual depiction (as such term is used in section
18 1460 of title 18, United States Code).

19 **SEC. 102. DATA MINIMIZATION.**

20 (a) IN GENERAL.—A covered entity may not collect,
21 process, retain, or transfer covered data of an individual
22 or direct a service provider to collect, process, retain, or
23 transfer covered data of an individual beyond what is nec-
24 essary, proportionate, and limited—

25 (1) to provide or maintain—

1 (A) a specific product or service requested
2 by the individual to whom the data pertains, in-
3 cluding any associated routine administrative,
4 operational, or account-servicing activity, such
5 as billing, shipping, delivery, storage, or ac-
6 counting; or

7 (B) a communication, that is not an adver-
8 tisement, by the covered entity to the individual
9 reasonably anticipated within the context of the
10 relationship; or

11 (2) for a purpose expressly permitted under
12 subsection (d).

13 (b) ADDITIONAL PROTECTIONS FOR SENSITIVE COV-
14 ERED DATA.—Subject to subsection (a) and unless for a
15 purpose expressly permitted by paragraph (2), (3), (4),
16 (5), (6), (8), (9), (11), (12), or (13) of subsection (d),
17 a covered entity may not transfer sensitive covered data
18 to a third party or direct a service provider to transfer
19 sensitive covered data to a third party without the affirma-
20 tive express consent of the individual to whom such data
21 pertains.

22 (c) ADDITIONAL PROTECTIONS FOR BIOMETRIC IN-
23 FORMATION AND GENETIC INFORMATION.—

24 (1) COLLECTION.—Subject to subsection (a), a
25 covered entity may not collect biometric information

1 or genetic information or direct a service provider to
2 collect biometric information or genetic information
3 without the affirmative express consent of the indi-
4 vidual to whom such information pertains.

5 (2) PROCESSING.—Subject to subsection (a), a
6 covered entity may not process biometric information
7 or genetic information or direct a service provider to
8 process biometric information or genetic information
9 without the affirmative express consent of the indi-
10 vidual to whom such information pertains, unless for
11 a purpose permitted by paragraph (2), (3), or (4) of
12 subsection (d).

13 (3) RETENTION.—Subject to subsection (a), a
14 covered entity may not retain biometric information
15 or direct a service provider to retain biometric infor-
16 mation beyond the point at which the purpose for
17 which an individual provided affirmative express
18 consent under paragraph (1) has been satisfied or
19 beyond the date that is 3 years after the date of the
20 last interaction of the individual with the covered en-
21 tity or service provider, whichever occurs first, un-
22 less for a purpose permitted under paragraph (2),
23 (3), or (4) of subsection (d).

24 (4) TRANSFER.—

1 (A) AFFIRMATIVE EXPRESS CONSENT RE-
2 QUIRED.—Subject to subsection (a), a covered
3 entity may not transfer biometric information
4 or genetic information to a third party or direct
5 a service provider to transfer biometric informa-
6 tion or genetic information to a third party
7 without the affirmative express consent of the
8 individual to whom such information pertains,
9 unless for a purpose permitted by paragraph
10 (2), (3), or (4) of subsection (d).

11 (B) NO TRANSFER FOR PAYMENT OR
12 OTHER VALUABLE CONSIDERATION.—A covered
13 entity may not transfer biometric information
14 or genetic information to a third party, or di-
15 rect a service provider to transfer biometric in-
16 formation or genetic information to a third
17 party for payment or other valuable consider-
18 ation (regardless of the purpose of the transfer,
19 including a purpose described in subparagraph
20 (A)).

21 (d) PERMITTED PURPOSES.—Subject to the require-
22 ments in subsections (b) and (c), a covered entity may
23 collect, process, retain, or transfer or direct a service pro-
24 vider to collect, process, retain, or transfer covered data
25 for the following purposes, if the covered entity or service

1 provider can demonstrate that the collection, processing,
2 retention, or transfer is necessary, proportionate, and lim-
3 ited to such purpose:

4 (1) To protect data security as described in sec-
5 tion 109, protect against spam, or protect and main-
6 tain networks and systems, including through
7 diagnostics, debugging, and repairs.

8 (2) To comply with a legal obligation imposed
9 by a Federal, State, Tribal, or local law that is not
10 preempted by this title.

11 (3) To investigate, establish, prepare for, exer-
12 cise, or defend cognizable legal claims of the covered
13 entity or service provider.

14 (4) To transfer covered data to a Federal,
15 State, Tribal, or local law enforcement agency pur-
16 suant to a lawful warrant, administrative subpoena,
17 or other form of lawful process.

18 (5) To effectuate a product recall pursuant to
19 Federal or State law, or to fulfill a warranty.

20 (6) To conduct market research.

21 (7) With respect to covered data previously col-
22 lected in accordance with this title, to process the
23 covered data such that the covered data becomes de-
24 identified data, including in order to—

1 (A) develop or enhance a product or serv-
2 ice of the covered entity or service provider;

3 (B) conduct research or analytics to im-
4 prove a product or service of the covered entity
5 or service provider;

6 (C) conduct research to improve the effec-
7 tiveness and safety of health care products and
8 treatments and medical devices;

9 (D) enable the effective delivery and ad-
10 ministration of healthcare products and treat-
11 ments to patients, in compliance with Federal
12 Regulations; or

13 (E) to monitor the safety and efficacy of
14 products and services administered to patients,
15 in compliance with Federal Regulations.

16 (8) To transfer assets to a third party in the
17 context of a merger, acquisition, bankruptcy, or
18 similar transaction, with respect to which the third
19 party assumes control, in whole or in part, of the as-
20 sets of the covered entity, but only if the covered en-
21 tity, in a reasonable time prior to such transfer, pro-
22 vides each affected individual with—

23 (A) a notice describing such transfer, in-
24 cluding the name of the entity or entities receiv-
25 ing the covered data of the individual and the

1 privacy policies of such entity or entities as de-
2 scribed in section 104; and

3 (B) a reasonable opportunity to—

4 (i) withdraw any previously provided
5 consent in accordance with the require-
6 ments of affirmative express consent under
7 this title related to the covered data of the
8 individual; and

9 (ii) request the deletion of the covered
10 data of the individual, as described in sec-
11 tion 105.

12 (9) With respect to a covered entity or service
13 provider that is a telecommunications carrier or a
14 provider of a mobile service, interconnected VoIP
15 service, or non-interconnected VoIP service (as such
16 terms are defined in section 3 of the Communica-
17 tions Act of 1934 (47 U.S.C. 153)), to provide call
18 location information in a manner described in sub-
19 paragraph (A) or (C) of section 222(d)(4) of such
20 Act (47 U.S.C. 222(d)(4)).

21 (10) To prevent, detect, protect against, inves-
22 tigate, or respond to fraud, excluding the transfer of
23 covered data for payment or other valuable consider-
24 ation to a government entity.

1 (11) To prevent, detect, protect against, inves-
2 tigate, or respond to an ongoing or imminent secu-
3 rity incident relating to network security or physical
4 security, including an intrusion or trespass, medical
5 alert or request for a medical response, fire alarm or
6 request for a fire response, or access control.

7 (12) To prevent, detect, protect against, or re-
8 spond to an imminent or ongoing public safety inci-
9 dent (such as a mass casualty event, natural dis-
10 aster, or national security incident), excluding the
11 transfer of covered data for payment or other valu-
12 able consideration to a government entity.

13 (13) Except with respect to health information,
14 to prevent, detect, protect against, investigate, or re-
15 spond to criminal activity or harassment, excluding
16 the transfer of covered data for payment or other
17 valuable consideration to a government entity.

18 (14) Except with respect to sensitive covered
19 data, and only with respect to covered data pre-
20 viously collected in accordance with this title, to
21 process or transfer such data to provide first-party
22 advertising or contextual advertising, or to measure
23 and report on marketing performance or media per-
24 formance by the covered entity, including processing
25 or transferring covered data for measurement and

1 reporting of frequency, attribution, and performance,
2 including by independent entities, except that this
3 paragraph does not permit the processing or trans-
4 fer of covered data for first-party advertising to a
5 covered minor, as prohibited pursuant to section
6 120.

7 (15) Except with respect to sensitive covered
8 data, and only with respect to covered data pre-
9 viously collected in accordance with this title, to
10 process or to transfer such data to provide targeted
11 advertising, direct mail targeted advertising, or
12 email targeted advertising (subject to 15 U.S.C. 103
13 and all regulations promulgated thereunder), or to
14 measure and report on marketing performance or
15 media performance, including processing or transfer-
16 ring covered data for measurement and reporting of
17 frequency, attribution, and performance, including
18 by independent entities, except that this paragraph
19 does not permit the processing or transfer of covered
20 data for targeted advertising to an individual who
21 has opted out of targeted advertising pursuant to
22 section 106, or to a covered minor as prohibited pur-
23 suant to section 120.

1 (16) To conduct a public or peer-reviewed sci-
2 entific, historical, or statistical research project
3 that—

4 (A) is in the public interest;

5 (B) adheres to all relevant laws and regu-
6 lations governing such research, including regu-
7 lations for the protection of human subjects, if
8 applicable;

9 (C) limits transfers to third parties of sen-
10 sitive covered data to only those transfers nec-
11 essary, proportionate, and limited to carry out
12 the research; and

13 (D) prohibits the transfer of covered data
14 to a data broker.

15 (17) Conduct medical research in compliance
16 with 45 CFR part 46 or 21 CFR parts 6, 50 and
17 56.

18 (e) GUIDANCE.—The Commission shall issue guid-
19 ance regarding what is necessary, proportionate, and lim-
20 ited to comply with this section.

21 (f) JOURNALISM.—Nothing in this title may be con-
22 strued to limit or diminish journalism, including the gath-
23 ering, preparing, collecting, photographing, recording,
24 writing, editing, reporting, or investigating news or infor-
25 mation that concerns local, national, or international

1 events or other matters of public interest for dissemination
2 to the public.

3 **SEC. 103. PRIVACY BY DESIGN.**

4 (a) IN GENERAL.—Each covered entity and service
5 provider, shall establish, implement, and maintain reason-
6 able policies, practices, and procedures that reflect the role
7 of the covered entity or service provider, in the collection,
8 processing, retention, and transferring of covered data.

9 (b) REQUIREMENTS.—The policies, practices, and
10 procedures required by subsection (a) shall—

11 (1) identify, assess, and mitigate privacy risks
12 related to covered minors (including, if applicable, in
13 a manner that considers the developmental needs of
14 different age ranges of covered minors), people living
15 with disabilities, and individuals over the age of 65;

16 (2) mitigate privacy risks related to the prod-
17 ucts and services of the covered entity or service pro-
18 vider, including in the design, development, and im-
19 plementation of such products and services, taking
20 into account the role of the covered entity or service
21 provider and the information available to the covered
22 entity or service provider; and

23 (3) implement reasonable internal training and
24 safeguards to promote compliance with this title and
25 to mitigate privacy risks taking into account the role

1 of the covered entity or service provider and the in-
2 formation available to the covered entity or service
3 provider.

4 (c) FACTORS TO CONSIDER.—The policies, practices,
5 and procedures established by a covered entity or service
6 provider under subsection (a) shall align with, as applica-
7 ble—

8 (1) the nature, scope, and complexity of the ac-
9 tivities engaged in by the covered entity or service
10 provider, including whether the covered entity or
11 service provider, is a large data holder, nonprofit or-
12 ganization, or data broker, taking into account the
13 role of the covered entity or service provider and the
14 information available to the covered entity or service
15 provider;

16 (2) the sensitivity of the covered data collected,
17 processed, retained, or transferred by the covered
18 entity or service provider;

19 (3) the volume of covered data collected, proc-
20 essed, retained, or transferred by the covered entity
21 or service provider;

22 (4) the number of individuals and devices to
23 which the covered data collected, processed, retained,
24 or transferred by the covered entity or service pro-
25 vider;

1 (5) state-of-the-art administrative, techno-
2 logical, and organizational measures that, by default,
3 serve the purpose of protecting the privacy and secu-
4 rity of covered data as required by this title; and

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

8 (d) COMMISSION GUIDANCE.—Not later than 1 year
9 after the date of the enactment of this Act, the Commis-
10 sion shall issue guidance with respect to what constitutes
11 reasonable policies, practices, and procedures as required
12 by subsection (a). In issuing such guidance, the Commis-
13 sion shall consider unique circumstances applicable to non-
14 profit organizations, service providers, and data brokers.

15 **SEC. 104. TRANSPARENCY.**

16 (a) IN GENERAL.—Each covered entity and service
17 provider shall make publicly available, in a clear and con-
18 spicuous, not misleading, and easy-to-read a privacy policy
19 that provides a detailed and accurate representation of the
20 data collection, processing, retention, and transfer activi-
21 ties of the covered entity or service provider.

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

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

3 (A) the covered entity or service provider
4 to which the privacy policy applies, including a
5 point of contact and a monitored email address
6 or other monitored online contact mechanism,
7 as applicable, specific to data privacy and data
8 security inquiries; and

9 (B) any affiliate within the same corporate
10 structure as the covered entity or service pro-
11 vider, to which the covered entity or service pro-
12 vider may transfer data, that—

13 (i) is not under common branding
14 with the covered entity or service provider;
15 or

16 (ii) has different contact information
17 than the covered entity or service provider.

18 (2) With respect to the collection, processing,
19 and retention of covered data—

20 (A) the categories of covered data the cov-
21 ered entity or service provider collects, proc-
22 esses, or retains; and

23 (B) the processing purposes for each such
24 category of covered data.

1 (3) Whether the covered entity or service pro-
2 vider transfers covered data and, if so—

3 (A) each category of service provider or
4 third party to which the covered entity or serv-
5 ice provider transfers covered data;

6 (B) the name of each data broker to which
7 the covered entity or service provider transfers
8 covered data; and

9 (C) the purposes for which such data is
10 transferred.

11 (4) The length of time the covered entity or
12 service provider intends to retain each category of
13 covered data or, if it is not possible to identify the
14 length of time, the criteria used to determine the
15 length of time the covered entity or service provider
16 intends to retain each category of covered data.

17 (5) A prominent description of how an indi-
18 vidual may exercise the rights, as applicable, of the
19 individual under this title.

20 (6) A description of how a covered entity treats
21 data collected from covered minors differently than
22 it treats data collected from other individuals, when
23 the covered entity has knowledge that it has col-
24 lected data from covered minors.

1 (7) A general description of the data security
2 practices of the covered entity or service provider.

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

4 (9) Whether any covered data collected by the
5 covered entity or service provider is transferred to,
6 processed in, retained in, or otherwise accessible to
7 a foreign adversary (as determined by the Secretary
8 of Commerce and specified in section 7.4 of title 15,
9 Code of Federal Regulations, or any successor regu-
10 lation).

11 (c) LANGUAGES.—A privacy policy required under
12 subsection (a) shall be made available to the public in the
13 ten most used languages in which a covered entity pro-
14 vides products or services, or carries out activities related
15 to such product or service, or if the entity provides prod-
16 ucts or services in less than 10 languages, is provided in
17 the number of languages in which the covered entity pro-
18 vides a product or service, or carries out activities related
19 to such product or service.

20 (d) ACCESSIBILITY.—A covered entity or service pro-
21 vider shall provide the disclosures required under this sec-
22 tion in a manner that is reasonably accessible to and usa-
23 ble by individuals living with disabilities.

24 (e) MATERIAL CHANGES.—

1 (1) NOTICE AND OPT OUT.—A covered entity
2 that makes a material change to the privacy policy
3 or practices of the covered entity shall—

4 (A) provide to each affected individual, in
5 a clear and conspicuous manner—

6 (i) advance notice of such material
7 change; and

8 (ii) a means to opt out of the collec-
9 tion, retention processing or transfer of
10 any covered data of such individual pursu-
11 ant to such material change; and

12 (B) with respect to the covered data of any
13 individual who opts out using the means de-
14 scribed in subparagraph (A)(ii), discontinue the
15 collection, processing, retention, or transfer of
16 such covered data, unless such, processing, or
17 transfer is necessary, proportionate, and limited
18 to provide or maintain a product or service spe-
19 cifically requested by the individual.

20 (2) DIRECT NOTIFICATION.—A covered entity
21 shall take all reasonable electronic measures to pro-
22 vide direct notification, if possible, to each affected
23 individual regarding material changes to the privacy
24 policy of the entity, and such notification shall be
25 provided in each language in which the privacy pol-

1 icy is made available, taking into account available
2 technology and the nature of the relationship be-
3 tween the entity and the individual.

4 (3) CLARIFICATION.—Except as provided in
5 paragraph (1)(B), nothing in this subsection may be
6 construed to affect the requirements for covered en-
7 tities under sections 102, 105, and 106.

8 (f) TRANSPARENCY REQUIREMENTS FOR LARGE
9 DATA HOLDERS.—

10 (1) RETENTION OF PRIVACY POLICIES; LOG OF
11 MATERIAL CHANGES.—

12 (A) IN GENERAL.—Beginning not later
13 than 90 days after the date of the enactment of
14 this Act, each large data holder shall—

15 (i) retain and publish on the website
16 of the large data holder a copy of each
17 version of the privacy policy of the large
18 data holder required under subsection (a)
19 for not less than 10 years; and

20 (ii) make publicly available on the
21 website of the large data holder, in a clear
22 and conspicuous manner, a log that de-
23 scribes the date and nature of each mate-
24 rial change to the privacy policy of the
25 large data holder during the preceding 10-

1 year period in a manner that is sufficient
2 for a reasonable individual to understand
3 the effect of each material change.

4 (B) EXCLUSION.—This paragraph does not
5 apply to material changes to previous versions
6 of the privacy policy of a large data holder that
7 precede the date of the enactment of this Act.

8 (2) SHORT FORM NOTICE TO CONSUMERS.—

9 (A) IN GENERAL.—In addition to the pri-
10 vacy policy required under subsection (a), a
11 large data holder shall provide a short-form no-
12 tice of the covered data practices of the large
13 data holder in a manner that—

14 (i) is concise;

15 (ii) is clear and conspicuous;

16 (iii) is readily accessible to an indi-
17 vidual, based on the manner in which the
18 individual interacts with the large data
19 holder and the products or services of the
20 large data holder and what is reasonably
21 anticipated within the context of the rela-
22 tionship between the individual and the
23 large data holder;

24 (iv) includes an overview of individual
25 rights and disclosures to reasonably draw

1 attention to data practices that may be un-
2 expected or that involve sensitive covered
3 data; and

4 (v) is not more than 500 words in
5 length in the English language or not more
6 than 550 words in length if in a language
7 other than English.

8 (B) GUIDANCE.—Not later than 180 days
9 after the date of the enactment of this Act, the
10 Commission shall issue guidance establishing
11 the minimum data disclosures necessary for the
12 short-form notice described in this paragraph
13 and shall include templates or models for such
14 notice.

15 **SEC. 105. INDIVIDUAL CONTROL OVER COVERED DATA.**

16 (a) ACCESS TO, AND CORRECTION, DELETION, AND
17 PORTABILITY OF, COVERED DATA.—After receiving a
18 verified request from an individual, including from a par-
19 ent acting on behalf of a child, a covered entity shall pro-
20 vide the individual with the right to—

21 (1) access—

22 (A) in a format that can be naturally read
23 by a human, the covered data of the individual
24 (or an accurate representation of the covered
25 data of the individual or of the child, in the

1 case of parental access, if the covered data is no
2 longer in the possession of the covered entity or
3 a service provider acting on behalf of the cov-
4 ered entity) that is collected, processed, or re-
5 tained by the covered entity or any service pro-
6 vider of the covered entity;

7 (B) the name of any third party or service
8 provider to whom the covered entity has trans-
9 ferred the covered data, as well as the cat-
10 egories of sources from which the covered data
11 was collected; and

12 (C) a description of the purpose for which
13 the covered entity transferred any covered data
14 of the individual or of the child, in the case of
15 parental access, to a third party or service pro-
16 vider;

17 (2) correct any inaccuracy or incomplete infor-
18 mation with respect to the covered data of the indi-
19 vidual or of the child, in the case of parental re-
20 quest, that is collected, processed, or retained by the
21 covered entity and, for covered data that has been
22 transferred, request the covered entity to notify any
23 third party or service provider to which the covered
24 entity transferred such covered data of the corrected

1 information so that service providers may provide
2 the assistance required by section 111(a)(1)(C);

3 (3) delete covered data of the individual or of
4 the child , in the case of parental request, that is re-
5 tained by the covered entity and, for covered data
6 that has been transferred, request that the covered
7 entity notify any third party or service provider to
8 which the covered entity transferred such covered
9 data of the deletion request of the individual or of
10 the child, so that service providers may provide the
11 assistance required by section 111(a)(1)(C);

12 (4) to the extent technically feasible, export cov-
13 ered data of the individual or of the child, in the
14 case of parental request, that is collected, processed,
15 or retained by the covered entity, without licensing
16 restrictions that unreasonably limit such transfers,
17 in—

18 (A) a format that can be naturally read by
19 a human; and

20 (B) a format that is portable, structured,
21 interoperable, and machine-readable; and

22 (5) if the individual is a covered minor, delete
23 covered data collected from the covered minor or
24 content or information submitted by the covered
25 minor to a covered entity.

1 (b) FREQUENCY AND COST.—A covered entity—

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

5 (2) with respect to—

6 (A) the first 3 instances that an individual
7 exercises any right described in subsection (a)
8 during any 12-month period, shall allow the in-
9 dividual to exercise such right free of charge;
10 and

11 (B) any instance beyond the first 3 in-
12 stances described in subparagraph (A), may
13 charge a reasonable fee for each additional re-
14 quest to exercise any such right during such
15 12-month period.

16 (c) TIMING.—

17 (1) IN GENERAL.—Subject to subsections (b),
18 (d), and (e), each request under subsection (a) shall
19 be completed—

20 (A) by any covered entity that is a large
21 data holder or data broker, not later than 30
22 calendar days of such request of an individual,
23 unless it is impossible or demonstrably imprac-
24 ticable to verify the individual; or

1 (B) by a covered entity that is not a large
2 data holder or data broker, not later than 45
3 calendar days of such request from an indi-
4 vidual, unless it is impossible or demonstrably
5 impracticable to verify the individual.

6 (2) EXTENSION.—The response period required
7 under paragraph (1) may be extended once, by not
8 more than the applicable time period described in
9 such paragraph, when reasonably necessary, consid-
10 ering the complexity and number of requests from
11 the individual, if the covered entity informs the indi-
12 vidual of any such extension within the initial re-
13 sponse period and the reason for the extension.

14 (d) VERIFICATION.—

15 (1) IN GENERAL.—A covered entity shall rea-
16 sonably verify that an individual making a request
17 to exercise a right described in subsection (a) is—

18 (A) the individual whose covered data is
19 the subject of the request;

20 (B) the parent of a child whose covered
21 data, or with respect to paragraph (5) content
22 or other information, is the subject of the re-
23 quest; or

24 (C) another individual, that is not an enti-
25 ty, on behalf of an individual. authorized to

1 make such a request on behalf of the individual
2 whose covered data is the subject of the re-
3 quest.

4 (2) ADDITIONAL INFORMATION.—If a covered
5 entity cannot make the verification described in
6 paragraph (1), the covered entity—

7 (A) may request that the individual mak-
8 ing the request provide any additional informa-
9 tion necessary for the sole purpose of verifying
10 the identity of the individual, and in the case of
11 a parent, that the person making the request is
12 the parent of the child whose information is at
13 issue, except that the request of the covered en-
14 tity may not be burdensome on the individual;
15 and

16 (B) may not process, retain, or transfer
17 such additional information for any other pur-
18 pose.

19 (e) EXCEPTIONS.—

20 (1) REQUIRED EXCEPTIONS.—A covered entity
21 may not permit an individual to exercise a right de-
22 scribed in subsection (a) in whole or in part, if the
23 covered entity—

24 (A) cannot reasonably verify that the indi-
25 vidual making such request is the individual

1 whose covered data is the subject of the re-
2 quest, or the parent of a child whose covered
3 data is the subject of the request, or another
4 person authorized to make such a request on
5 behalf of the individual whose covered data, or
6 with respect to paragraph (5) content or other
7 information, is the subject of the request;

8 (B) determines that exercise of the right
9 would require access to, or the correction or de-
10 letion of, the sensitive covered data of an indi-
11 vidual other than the individual whose covered
12 data is the subject of the request;

13 (C) determines that exercise of the right
14 would require correction or deletion of covered
15 data subject to a warrant, lawfully executed
16 subpoena, or litigation or equivalent preserva-
17 tion notice, or hold notice in connection with
18 such warrant or subpoena or issued in a matter
19 in which the covered entity is a named party;

20 (D) determines that exercise of the right
21 would violate a Federal, State, Tribal, or local
22 law that is not preempted by this title;

23 (E) determines that exercise of the right
24 would violate the professional ethical obligations
25 of the covered entity;

1 (F) reasonably believes that the request is
2 made to further fraud;

3 (G) except with respect to health informa-
4 tion, reasonably believes that the request is
5 made in furtherance of criminal activity; or

6 (H) reasonably believes that complying
7 with the request would threaten data security
8 or network security.

9 (2) PERMISSIVE EXCEPTIONS.—A covered enti-
10 ty may decline, with adequate explanation to the in-
11 dividual making the request, to comply with a re-
12 quest to exercise a right described in subsection (a),
13 in whole or in part, that would—

14 (A) be demonstrably impracticable due to
15 technological limitations or prohibitive cost, and
16 if the covered entity provides a detailed descrip-
17 tion to the individual regarding the inability to
18 comply with the request due to technological
19 limitations or prohibitive cost;

20 (B) delete covered data necessary to per-
21 form a contract between the covered entity and
22 the individual;

23 (C) with respect to a right described in
24 paragraph (1) or (4) of subsection (a), require
25 the covered entity to release trade secrets or

1 other privileged, proprietary, or confidential
2 business information;

3 (D) prevent a covered entity from being
4 able to maintain a confidential record of opt-out
5 requests pursuant to this title that is main-
6 tained solely for the purpose of preventing cov-
7 ered data of an individual from being collected,
8 processed, retained, or transferred after the in-
9 dividual submits an opt-out request;

10 (E) with respect to a deletion request, re-
11 quire a private elementary or secondary school
12 (as defined by State law) or a private institu-
13 tion of higher education (as defined in title I of
14 the Higher Education Act of 1965 (20 U.S.C.
15 1001 et seq.)) to delete covered data, if the de-
16 letion would unreasonably interfere with the
17 provision of education services by, or the ordi-
18 nary operation of, the school or institution;

19 (F) delete covered data that relates to a
20 public figure regarding a matter of legitimate
21 public interest and for which the requesting in-
22 dividual has no reasonable expectation of pri-
23 vacy; or

24 (G) delete covered data that the covered
25 entity reasonably believes may be evidence of an

1 abuse of the covered entity's products or serv-
2 ices, including violations of terms of service.

3 (3) RULE OF CONSTRUCTION.—This section
4 may not be construed to require a covered entity or
5 service provider acting on behalf of a covered entity
6 to—

7 (A) retain covered data collected for a sin-
8 gle, 1-time transaction, if such covered data is
9 not processed or transferred by the covered en-
10 tity for any purpose other than completing such
11 transaction;

12 (B) re-identify or attempt to re-identify de-
13 identified data; or

14 (C) collect or retain any data in order to
15 be capable of associating a request with the cov-
16 ered data that is the subject of the request.

17 (4) PARTIAL COMPLIANCE.—In the event a cov-
18 ered entity declines a request under paragraph (2),
19 the covered entity shall comply with the remainder
20 of the request if partial compliance is possible and
21 not unduly burdensome.

22 (5) NUMBER OF REQUESTS.—For purposes of
23 paragraph (2)(A), the receipt of a large number of
24 verified requests, on its own, may not be considered

1 to render compliance with a request demonstrably
2 impracticable.

3 (6) ADDITIONAL EXCEPTIONS.—

4 (A) IN GENERAL.—The Commission may
5 promulgate regulations, in accordance with sec-
6 tion 553 of title 5, United States Code, to es-
7 tablish additional permissive exceptions to sub-
8 section (a) necessary to protect the rights of in-
9 dividuals, to alleviate undue burdens on covered
10 entities, to prevent unjust or unreasonable out-
11 comes from the exercise of access, correction,
12 deletion, or portability rights, or as otherwise
13 necessary to fulfill the purposes of this section.

14 (B) CONSIDERATIONS.—In establishing
15 any exceptions under subparagraph (A), the
16 Commission shall consider any relevant changes
17 in technology, means for protecting privacy and
18 other rights, and beneficial uses of covered data
19 by covered entities.

20 (C) CLARIFICATION.—A covered entity
21 may decline to comply with a request of an in-
22 dividual to exercise a right under this section
23 pursuant to an exception the Commission estab-
24 lishes under this paragraph.

1 (f) LARGE DATA HOLDER METRICS REPORTING.—

2 With respect to each calendar year for which an entity
3 is a large data holder, such entity shall comply with the
4 following requirements:

5 (1) REQUIRED METRICS.—Compile the fol-
6 lowing information for such calendar year:

7 (A) The number of verified access requests
8 under subsection (a)(1).

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

11 (C) The number of verified deletion re-
12 quests under subsection (a)(5).

13 (D) The number of verified requests to opt
14 out of covered data transfers under section
15 106(a)(1).

16 (E) The number of verified requests to opt
17 out of targeted advertising under section
18 106(a)(2).

19 (F) For each category of request described
20 in subparagraphs (A) through (E), the number
21 of such requests that the large data holder com-
22 plied with in whole or in part.

23 (G) For each category of request described
24 in subparagraphs (A) through (E), the average

1 number of days within which the large data
2 holder substantively responded to the requests.

3 (2) PUBLIC DISCLOSURE.—Disclose, not later
4 than July 1 of each calendar year, the information
5 compiled under paragraph (1) for the previous cal-
6 endar year—

7 (A) in the privacy policy of the large data
8 holder; or

9 (B) on a publicly available website of the
10 large data holder that is accessible from a
11 hyperlink included in the privacy policy.

12 (g) GUIDANCE.—Not later than 1 year after the date
13 of the enactment of this Act, the Commission shall issue
14 guidance to clarify or explain the provisions of this section
15 and establish practices by which a covered entity may
16 verify a request to exercise a right described in subsection
17 (a).

18 (h) ACCESSIBILITY.—

19 (1) LANGUAGE.—A covered entity shall facili-
20 tate the ability of individuals to make requests to ex-
21 ercise rights described in subsection (a) in any lan-
22 guage in which the covered entity provides a product
23 or service.

24 (2) INDIVIDUALS LIVING WITH DISABILITIES.—
25 The mechanisms by which a covered entity enables

1 individuals to make a request to exercise a right de-
2 scribed in subsection (a) shall be readily accessible
3 and usable by individuals living with disabilities.

4 **SEC. 106. OPT-OUT RIGHTS AND UNIVERSAL MECHANISM.**

5 (a) IN GENERAL.—A covered entity shall provide to
6 an individual the following opt-out rights with respect to
7 the covered data of the individual:

8 (1) RIGHT TO OPT OUT OF COVERED DATA
9 TRANSFERS TO THIRD PARTIES.—A covered entity—

10 (A) shall provide an individual with a clear
11 and conspicuous means to opt out of the trans-
12 fer of the covered data of the individual to a
13 third party;

14 (B) upon establishment of an opt out
15 mechanism that meets the requirements and
16 technical specifications promulgated under sub-
17 section (b), shall allow an individual to make an
18 opt-out designation pursuant to subparagraph
19 (A) through the opt out mechanism;

20 (C) shall abide by an opt-out designation
21 made pursuant to subparagraph (A) and com-
22 municate such designation to all relevant serv-
23 ice providers and third parties; and

24 (D) except as provided in section
25 112(c)(3), need not allow an individual to opt

1 out of a transfer of covered data made pursuant
2 to a permissible purpose described in paragraph
3 (1), (2), (3), (4), (5), (6), (7), (8), (9), (10),
4 (11), (12), (13), or (14) of section 102(d).

5 (2) RIGHT TO OPT OUT OF TARGETED ADVER-
6 TISING.—A covered entity that engages in targeted
7 advertising shall—

8 (A) provide an individual with a clear and
9 conspicuous means to opt out of the processing
10 and transfer of covered data of the individual in
11 furtherance of targeted advertising;

12 (B) upon establishment of an opt out
13 mechanism that meets the requirements and
14 technical specifications promulgated under sub-
15 section (b), allow an individual to make an opt-
16 out designation with respect to targeted adver-
17 tising through the opt-out mechanism; and

18 (C) abide by any such opt-out designation
19 made by an individual and communicate such
20 designation to all relevant service providers and
21 third parties.

22 (b) UNIVERSAL OPT-OUT MECHANISMS.—

23 (1) IN GENERAL.—Not later than 2 years after
24 the date of the enactment of this Act, the Commis-
25 sion shall, in consultation with the Secretary of

1 Commerce, promulgate regulations, in accordance
2 with section 553 of title 5, United States Code, to
3 establish requirements and technical specifications
4 for one or more opt out mechanisms (including glob-
5 al privacy signals, such as browser or device privacy
6 settings) for individuals to exercise the opt-out
7 rights established under this title through a single
8 interface that—

9 (A) ensures that the opt-out preference
10 signal—

11 (i) is user-friendly, clearly described,
12 and easy-to-use by a reasonable individual;

13 (ii) does not require that an individual
14 provide additional information beyond what
15 is necessary to indicate such preference;

16 (iii) clearly represents the preference
17 of an individual;

18 (iv) is provided in the ten most used
19 languages in which a covered entity pro-
20 vides products or services subject to the
21 opt out, or if the entity provides products
22 or services in less than 10 languages, is
23 provided in the number of languages in
24 which the covered entity provides a product
25 or service; and

1 (v) is provided in a manner that is
2 reasonably accessible to and usable by indi-
3 viduals living with disabilities;

4 (B) provides a mechanism for an individual
5 to selectively opt out of the collection, proc-
6 essing, retention, or transfer of covered data by
7 a covered entity, without affecting the pref-
8 erences of the individual with respect to other
9 entities or disabling the opt-out preference sig-
10 nal globally;

11 (C) states that, in the case of a page or
12 setting view that the individual accesses to set
13 the opt-out preference signal, the individual
14 should see up to 2 choices, corresponding to the
15 rights established under subsection (a); and

16 (D) ensures that the opt-out preference
17 signal will be registered and set only by the in-
18 dividual or another individual, that is not an
19 entity, on behalf of an individual.

20 (2) EFFECT OF DESIGNATIONS.—A covered en-
21 tity shall abide by any designation made by an indi-
22 vidual through any mechanism that meets the re-
23 quirements and technical specifications promulgated
24 under paragraph (1).

1 **SEC. 107. INTERFERENCE WITH CONSUMER RIGHTS.**

2 (a) DARK PATTERNS PROHIBITED.—

3 (1) IN GENERAL.—A covered entity may not
4 use dark patterns to—

5 (A) divert the attention of an individual
6 from any notice required under this title;

7 (B) impair the ability of an individual to
8 exercise any right under this title; or

9 (C) obtain, infer, or facilitate the consent
10 of an individual for any action that requires the
11 consent of an individual under this title.

12 (2) CLARIFICATION.—Any agreement by an in-
13 dividual that is obtained, inferred, or facilitated
14 through dark patterns does not constitute consent
15 for any purpose under this title.

16 (b) INDIVIDUAL AUTONOMY.—A covered entity may
17 not condition, effectively condition, attempt to condition,
18 or attempt to effectively condition the exercise of a right
19 described in this title through the use of any false, ficti-
20 tious, fraudulent, or materially misleading statement or
21 representation.

22 **SEC. 108. PROHIBITION ON DENIAL OF SERVICE AND WAIV-
23 ER OF RIGHTS.**

24 (a) RETALIATION THROUGH SERVICE OR PRICING
25 PROHIBITED.—A covered entity may not retaliate against
26 an individual for exercising any of the rights guaranteed

1 by this title, or any regulations promulgated under this
2 title, including by denying goods or services, charging dif-
3 ferent prices or rates for goods or services, or providing
4 a different level of quality of goods or services.

5 (b) RULES OF CONSTRUCTION.—

6 (1) BONA FIDE LOYALTY PROGRAMS.—

7 (A) IN GENERAL.—Nothing in subsection
8 (a) may be construed to prohibit a covered enti-
9 ty from offering—

10 (i) a different price, rate, level, qual-
11 ity, or selection of goods or services, or
12 functionalities, to an individual, including
13 offering goods or services for no fee, if the
14 offering is in connection with the voluntary
15 participation of the individual in a bona
16 fide loyalty program, and if—

17 (I) the individual provided af-
18 firmative express consent to partici-
19 pate in such bona fide loyalty pro-
20 gram;

21 (II) the covered entity abides by
22 the exercise by the individual of any
23 right provided by subsection (b) or (c)
24 of section 102, section 105, or section
25 106; and

1 (III) the sale of covered data is
2 not a condition of participation in the
3 bona fide loyalty program; or

4 (ii) different prices, rates, levels,
5 qualities, or selection of goods or services,
6 or functionalities with respect to a product
7 or service based on the decision of an indi-
8 vidual to terminate membership in a bona
9 fide loyalty program or to exercise a right
10 under section 105(a)(3) to delete covered
11 data that is necessary for participation in
12 the bona fide loyalty program.

13 (B) BONA FIDE LOYALTY PROGRAM DE-
14 FINED.—For purposes of this section, the term
15 “bona fide loyalty program” includes rewards,
16 premium features, discounts, and club card pro-
17 grams offered by a covered entity that is not a
18 covered high-impact social media company or
19 data broker.

20 (2) MARKET RESEARCH.—Nothing in sub-
21 section (a) may be construed to prohibit a covered
22 entity from offering a financial incentive or other
23 consideration to an individual for participation in
24 market research.

1 (3) DECLINING A PRODUCT OR SERVICE.—
2 Nothing in subsection (a) may be construed to pro-
3 hibit a covered entity from declining to provide a
4 product or service or a bona fide loyalty program, if
5 the collection, processing, retention, or transfer af-
6 fected by the relevant individual exercising a right
7 guaranteed by this title is necessary, proportionate,
8 and limited to providing such product or service.

9 **SEC. 109. DATA SECURITY AND PROTECTION OF COVERED**
10 **DATA.**

11 (a) ESTABLISHMENT OF DATA SECURITY PRAC-
12 TICES.—

13 (1) IN GENERAL.—Each covered entity or serv-
14 ice provider shall establish, implement, and maintain
15 reasonable data security practices to protect—

16 (A) the confidentiality, integrity, and avail-
17 ability of covered data; and

18 (B) covered data against unauthorized ac-
19 cess.

20 (2) CONSIDERATIONS.—The data security prac-
21 tices required under paragraph (1) shall be appro-
22 priate to—

23 (A) the size and complexity of the covered
24 entity or service provider;

1 (B) the nature and scope of the relevant
2 collecting, processing, retaining, or transferring
3 of covered data, taking into account changing
4 business operations with respect to covered
5 data;

6 (C) the volume, nature, and sensitivity of
7 the covered data; and

8 (D) the state-of-the-art (and limitations
9 thereof) in administrative, technical, and phys-
10 ical safeguards for protecting covered data.

11 (b) SPECIFIC REQUIREMENTS.—The data security
12 practices required under subsection (a) shall include, at
13 a minimum, the following:

14 (1) ASSESS VULNERABILITIES.—Routinely iden-
15 tifying and assessing any reasonably foreseeable in-
16 ternal or external risk to, or vulnerability in, each
17 system maintained by the covered entity or service
18 provider that collects, processes, retains, or transfers
19 covered data, including unauthorized access to or
20 corruption of such covered data, human
21 vulnerabilities, access rights, and the use of service
22 providers. Such activities shall include developing
23 and implementing a plan for receiving and consid-
24 ering unsolicited reports of vulnerability by any enti-
25 ty or individual and, if such a report is reasonably

1 credible, performing a reasonable and timely inves-
2 tigation of such report and taking appropriate action
3 to protect covered data against the vulnerability.

4 (2) PREVENTIVE AND CORRECTIVE ACTION.—

5 (A) IN GENERAL.—Taking preventive and
6 corrective action to mitigate any reasonably
7 foreseeable internal or external risk to, or vul-
8 nerability of, covered data identified by the cov-
9 ered entity or service provider, consistent with
10 the nature of such risk or vulnerability and the
11 role of the covered entity or service provider in
12 collecting, processing, retaining, or transferring
13 the data, which may include implementing ad-
14 ministrative, technical, or physical safeguards
15 or changes to data security practices or the ar-
16 chitecture, installation, or implementation of
17 network or operating software.

18 (B) EVALUATION OF PREVENTATIVE AND
19 CORRECTIVE ACTION.—Evaluating and making
20 reasonable adjustments to the action described
21 in subparagraph (A) in light of any material
22 changes in state-of-the-art technology, internal
23 or external threats to covered data, and chang-
24 ing business operations with respect to covered
25 data.

1 (3) INFORMATION RETENTION AND DIS-
2 POSAL.—Disposing of covered data (either by or at
3 the direction of the covered entity) that is required
4 to be deleted by law or is no longer necessary for the
5 purpose for which the data was collected, processed,
6 retained, or transferred, unless a permitted purpose
7 under section 102 applies, except that retention and
8 disposal of biometric information shall be governed
9 by section 102(c)(3). Such disposal shall include de-
10 stroying, permanently erasing, or otherwise modi-
11 fying the covered data to make such data perma-
12 nently unreadable or indecipherable and unrecover-
13 able to ensure ongoing compliance with this section.

14 (4) RETENTION SCHEDULE.—Developing, main-
15 taining, and adhering to a retention schedule for
16 covered data consistent with paragraph (3).

17 (5) TRAINING.—Training each employee with
18 access to covered data on how to safeguard covered
19 data, and updating such training as necessary.

20 (6) INCIDENT RESPONSE.—Implementing pro-
21 cedures to detect, respond to, and recover from data
22 security incidents, including breaches.

23 (c) REGULATIONS.—The Commission may, in con-
24 sultation with the Secretary of Commerce, promulgate, in
25 accordance with section 553 of title 5, United States Code,

1 technology-neutral, process-based regulations to carry out
2 this section.

3 **SEC. 110. EXECUTIVE RESPONSIBILITY.**

4 (a) DESIGNATION OF PRIVACY AND DATA SECURITY
5 OFFICERS.—

6 (1) IN GENERAL.—A covered entity or service
7 provider (except for a large data holder) shall des-
8 ignate 1 or more qualified employees to serve as pri-
9 vacy and data security officers.

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

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

18 (B) facilitate the ongoing compliance of
19 the covered entity or service provider with this
20 title.

21 (b) REQUIREMENTS FOR LARGE DATA HOLDERS.—

22 (1) DESIGNATION.—A covered entity or service
23 provider that is a large data holder shall designate
24 1 qualified employee to serve as a privacy officer and

1 1 qualified employee to serve as a data security offi-
2 cer.

3 (2) ANNUAL CERTIFICATION.—

4 (A) IN GENERAL.—Beginning on the date
5 that is 1 year after the date of the enactment
6 of this Act, the chief executive officer of a large
7 data holder (or, if the large data holder does
8 not have a chief executive officer, the highest
9 ranking officer of the large data holder) and
10 each privacy officer and data security officer of
11 such large data holder designated under para-
12 graph (1), shall annually certify to the Commis-
13 sion, in a manner specified by the Commission,
14 that the large data holder implements and
15 maintains—

16 (i) internal controls reasonably de-
17 signed, implemented, maintained, and
18 monitored to comply with this title; and

19 (ii) internal reporting structures (as
20 described in paragraph (3)) to ensure that
21 such certifying officers are involved in, and
22 responsible for, decisions that impact com-
23 pliance by the large data holder with this
24 title.

1 (B) REQUIREMENTS.—A certification sub-
2 mitted under subparagraph (A) shall be based
3 on a review of the effectiveness of the internal
4 controls and reporting structures of the large
5 data holder that is conducted by the certifying
6 officers not more than 90 days before the sub-
7 mission of the certification.

8 (3) INTERNAL REPORTING STRUCTURE RE-
9 QUIREMENTS.—At least 1 of the officers designated
10 under paragraph (1) shall, either directly or through
11 a supervised designee—

12 (A) establish practices to periodically re-
13 view and update, as necessary, the privacy and
14 security policies, practices, and procedures of
15 the large data holder;

16 (B) conduct biennial and comprehensive
17 audits to ensure the policies, practices, and pro-
18 cedures of the large data holder comply with
19 this title and, upon request, make such audits
20 available to the Commission;

21 (C) develop a program to educate and
22 train employees about the requirements of this
23 title;

24 (D) maintain updated, accurate, clear, and
25 understandable records of all significant privacy

1 and data security practices of the large data
2 holder; and

3 (E) serve as the point of contact between
4 the large data holder and enforcement authori-
5 ties.

6 (4) PRIVACY IMPACT ASSESSMENTS.—

7 (A) IN GENERAL.—Not later than 1 year
8 after the date of the enactment of this Act or
9 1 year after the date on which an entity first
10 meets the definition of the term “large data
11 holder”, whichever is earlier, and biennially
12 thereafter, each large data holder shall conduct
13 a privacy impact assessment that weighs the
14 benefits of the covered data collection, proc-
15 essing, retention, and transfer practices of the
16 entity against the potential adverse con-
17 sequences of such practices to individual pri-
18 vacy.

19 (B) ASSESSMENT REQUIREMENTS.—A pri-
20 vacy impact assessment required under sub-
21 paragraph (A) shall be—

22 (i) reasonable and appropriate in
23 scope given—

24 (I) the nature and volume of the
25 covered data collected, processed, re-

1 tained, or transferred by the large
2 data holder; and

3 (II) the potential risks posed to
4 the privacy of individuals by the col-
5 lection, processing, retention, and
6 transfer of covered data by the large
7 data holder;

8 (ii) documented in written form and
9 maintained by the large data holder for as
10 long as the relevant privacy policy is re-
11 quired to be retained under section
12 104(f)(1); and

13 (iii) approved by the privacy officer of
14 the large data holder.

15 (C) ADDITIONAL FACTORS TO INCLUDE IN
16 ASSESSMENT.—In assessing privacy risks for
17 purposes of an assessment conducted under
18 subparagraph (A), including significant risks of
19 harm to the privacy of an individual or the se-
20 curity of covered data, the large data holder
21 shall include reviews of the means by which
22 technologies, including blockchain and distrib-
23 uted ledger technologies and other emerging
24 technologies, including privacy enhancing tech-
25 nologies, are used to secure covered data.

1 **SEC. 111. SERVICE PROVIDERS AND THIRD PARTIES.**

2 (a) SERVICE PROVIDERS.—

3 (1) IN GENERAL.—A service provider that col-
4 lects, processes, retains, or transfers covered data on
5 behalf of or at the direction of a covered entity or
6 another service provider—

7 (A) shall adhere to the instructions of the
8 covered entity and collect, process, retain, or
9 transfer covered data only to the extent nec-
10 essary, proportionate, and limited to provide a
11 service requested by the covered entity, as set
12 out in the contract described in paragraph (2);

13 (B) may not collect, process, retain, or
14 transfer covered data if the service provider has
15 actual knowledge that the covered entity vio-
16 lated this title with respect to such data;

17 (C) shall assist the covered entity in ful-
18 filling the obligations of the covered entity to
19 respond to consumer rights requests pursuant
20 to this title by—

21 (i) providing appropriate technical and
22 organizational support, taking into account
23 the nature of the processing and the infor-
24 mation reasonably available to the service
25 provider, for the covered entity to comply
26 with such request for covered data; or

1 (ii) fulfilling a request by a covered
2 entity to execute a consumer rights request
3 that the covered entity has determined
4 should be compiled with, by either—

5 (I) complying with the request
6 pursuant to the covered entity's in-
7 structions; or

8 (II) providing written verification
9 to the covered entity that it does not
10 hold data related to the request, that
11 complying with the request would be
12 inconsistent with its legal obligations,
13 or that the request falls within an ex-
14 ception pursuant to this title;

15 (D) shall, upon the reasonable request of
16 the covered entity, make available to the cov-
17 ered entity all information necessary to dem-
18 onstrate the compliance of the service provider
19 with the requirements of this title;

20 (E) shall delete or return, as directed by
21 the covered entity, all covered data as soon as
22 practicable after the contractually agreed upon
23 end of the provision of services, unless the re-
24 tention by the service provider of covered data
25 is required by law;

1 (F) may engage another service provider
2 for purposes of processing or retaining covered
3 data on behalf of the covered entity only after
4 exercising reasonable care in selecting such
5 other service provider as required by subsection
6 (d), providing the covered entity with written
7 notice of the engagement, and pursuant to a
8 written contract that requires such other service
9 provider to satisfy the requirements of this title
10 with respect to covered data; and

11 (G) shall—

12 (i) allow and cooperate with reason-
13 able assessments by the covered entity at
14 least once annually; or

15 (ii) arrange for a qualified and inde-
16 pendent assessor to conduct an assessment
17 of the policies and technical and organiza-
18 tional measures of the service provider in
19 support of the obligations of the service
20 provider under this title at least once an-
21 nually, using an appropriate and accepted
22 control standard or framework and assess-
23 ment procedure for such assessments, and
24 report the results of such assessment to
25 the covered entity.

1 (2) CONTRACT REQUIREMENTS.—An entity may
2 only operate as a service provider pursuant to any
3 contract between a covered entity and a service pro-
4 vider. Such contract—

5 (A) shall govern the data processing proce-
6 dures of the service provider with respect to any
7 collection, processing, retention, or transfer per-
8 formed on behalf of the covered entity;

9 (B) shall clearly set forth—

10 (i) instructions for collecting, proc-
11 essing, retaining, or transferring data;

12 (ii) the nature and purpose of the col-
13 lection, processing, retention, or transfer;

14 (iii) the type of data subject to collec-
15 tion, processing, retention, or transfer;

16 (iv) the duration of the processing or
17 retention; and

18 (v) the rights and obligations of both
19 parties;

20 (C) may not relieve the covered entity or
21 service provider of any obligation under this
22 title; and

23 (D) shall prohibit—

24 (i) the collection, processing, reten-
25 tion, or transfer of covered data in a man-

1 ner that does not comply with the require-
2 ments of paragraph (1); and

3 (ii) combining covered data that the
4 service provider receives from or on behalf
5 of 1 covered entity with covered data that
6 the service provider receives from or on be-
7 half of another entity or collects from the
8 interaction of the service provider with an
9 individual, unless such combining is nec-
10 essary to effectuate a purpose described in
11 section 102(d), other than paragraph (7),
12 (14), (15), or (16) of such section, and is
13 otherwise permitted under the contract.

14 (b) THIRD PARTIES.—

15 (1) IN GENERAL.—A third party may not proc-
16 ess, retain, or transfer third-party data for a pur-
17 pose other than—

18 (A) in the case of sensitive covered data, a
19 purpose for which an individual gave affirma-
20 tive express consent pursuant to subsection (b)
21 or (c) of section 102;

22 (B) in the case of sensitive covered data
23 that does not require affirmative express con-
24 sent pursuant to subsection (b) of section 102,
25 a purpose for which the covered entity or serv-

1 ice provider made a disclosure pursuant to sec-
2 tion 104; or

3 (C) in the case of covered data that is not
4 sensitive covered data, a purpose for which the
5 covered entity or service provider made a disclo-
6 sure pursuant to section 104.

7 (2) CONTRACT REQUIREMENTS.—Before trans-
8 ferring covered data to a third party, a covered enti-
9 ty shall enter into a contract with the third party
10 that—

11 (A) identifies the purposes for which cov-
12 ered data is being transferred, consistent with
13 paragraph (1);

14 (B) specifies that the third party may only
15 use the covered data for such purposes;

16 (C) with respect to the covered data trans-
17 ferred, requires the third party to comply with
18 all applicable provisions of, and regulations pro-
19 mulgated under, this title;

20 (D) requires the third party to notify the
21 covered entity or service provider if the third
22 party makes a determination that the third
23 party can no longer meet the obligations of the
24 third party under this title; and

1 (E) grants the covered entity or service
2 provider the right, upon notice (including under
3 subparagraph (D)), to take reasonable and ap-
4 propriate steps to stop and remediate unauthor-
5 ized use of covered data by the third party.

6 (c) RULES OF CONSTRUCTION.—

7 (1) SUCCESSIVE ACTOR VIOLATIONS.—

8 (A) IN GENERAL.—With respect to a viola-
9 tion of this title by a service provider or third
10 party regarding covered data received by the
11 service provider or third party from a covered
12 entity or another service provider, the covered
13 entity or service provider that transferred such
14 covered data to the service provider or third
15 party may not be considered to be in violation
16 of this title if the covered entity or service pro-
17 vider transferred the covered data to the service
18 provider or third party in compliance with the
19 requirements of this title and, at the time of
20 transferring such covered data, the covered en-
21 tity or service provider did not have actual
22 knowledge, or reason to believe that the service
23 provider or third party intended to violate this
24 title.

1 (B) KNOWLEDGE OF VIOLATION.—A cov-
2 ered entity or service provider that transfers
3 covered data to a service provider or third party
4 and has actual knowledge, or reason to believe,
5 that such service provider or third party is vio-
6 lating, or is about to violate, the requirements
7 of this title shall immediately cease the transfer
8 of covered data to such service provider or third
9 party.

10 (2) PRIOR ACTOR VIOLATIONS.—An entity that
11 collects, processes, retains, or transfers covered data
12 in compliance with the requirements of this title may
13 not be considered to be in violation of this title as
14 a result of a violation by an entity from which it re-
15 ceives, or on whose behalf it collects, processes, re-
16 tains, or transfers, covered data.

17 (d) REASONABLE CARE.—

18 (1) SERVICE PROVIDER SELECTION.—A covered
19 entity or service provider shall exercise reasonable
20 care in selecting a service provider.

21 (2) TRANSFER TO THIRD PARTY.—A covered
22 entity or service provider shall exercise reasonable
23 care in deciding to transfer covered data to a third
24 party.

1 (3) GUIDANCE.—Not later than 2 years after
2 the date of the enactment of this Act, the Commis-
3 sion shall publish guidance regarding compliance
4 with this subsection.

5 (e) RULE OF CONSTRUCTION.—Solely for purposes of
6 this section, the requirements under this section for serv-
7 ice providers to contract with, assist, and follow the in-
8 structions of covered entities shall also apply to any entity
9 that collects, processes, retains, or transfers covered data
10 for the purpose of performing services on behalf of, or at
11 the direction of, a government entity, as though such gov-
12 ernment entity were a covered entity.

13 **SEC. 112. DATA BROKERS.**

14 (a) NOTICE.—A data broker shall—

15 (1) establish and maintain a publicly available
16 website; and

17 (2) place a clear and conspicuous, and not mis-
18 leading, notice on such publicly available website,
19 and any mobile application of the data broker,
20 that—

21 (A) states that the entity is a data broker;

22 (B) states that an individual may exercise
23 a right described in section 105 or 106, and in-
24 cludes a link or other tool to allow an individual
25 to exercise such right;

1 (C) includes a link to the website described
2 in subsection (c)(3);

3 (D) is reasonably accessible to and usable
4 by individuals living with disabilities; and

5 (E) is provided in any language in which
6 the data broker provides products or services.

7 (b) PROHIBITED PRACTICES.—A data broker may
8 not—

9 (1) advertise or market access to, or the trans-
10 fer of, covered data for the purposes of—

11 (A) stalking or harassing an individual; or

12 (B) engaging in fraud, identity theft, or
13 unfair or deceptive acts or practices; or

14 (2) misrepresent the business practices of the
15 data broker.

16 (c) DATA BROKER REGISTRATION.—

17 (1) IN GENERAL.—Not later than January 31
18 of each calendar year that follows a calendar year
19 during which an entity acted as a data broker with
20 respect to more than 5,000 individuals or devices
21 that identify or are linked or reasonably linkable to
22 an individual, such entity shall register with the
23 Commission in accordance with this subsection.

1 (2) REGISTRATION REQUIREMENTS.—In reg-
2 istering with the Commission as required under
3 paragraph (1), a data broker shall do the following:

4 (A) Pay to the Commission a registration
5 fee of \$100.

6 (B) Provide the Commission with the fol-
7 lowing information:

8 (i) The legal name and primary valid
9 physical postal address, email address, and
10 internet address of the data broker.

11 (ii) A description of the categories of
12 covered data the data broker collects, proc-
13 esses, retains, or transfers.

14 (iii) The contact information of the
15 data broker, including the name of a con-
16 tact person, a human-monitored telephone
17 number, a human-monitored e-mail ad-
18 dress, a website, and a physical mailing ad-
19 dress.

20 (iv) A link to a website through which
21 an individual may easily exercise the rights
22 described in sections 105 and 106.

23 (3) DATA BROKER REGISTRY.—

24 (A) ESTABLISHMENT.—The Commission
25 shall establish and maintain on a publicly avail-

1 able website a searchable list of data brokers
2 that are registered with the Commission under
3 this subsection.

4 (B) REQUIREMENTS.—The registry estab-
5 lished under subparagraph (A) shall—

6 (i) allow members of the public to
7 search for and identify data brokers;

8 (ii) include the information required
9 under paragraph (2)(B) for each data
10 broker;

11 (iii) include a mechanism by which an
12 individual, including a parent acting on be-
13 half of a child, may submit to all registered
14 data brokers a “Do Not Collect” request
15 that results in registered data brokers no
16 longer collecting covered data related to
17 such individual without the affirmative ex-
18 press consent of such individual; and

19 (iv) include a mechanism by which an
20 individual, including a parent acting on be-
21 half of a child, may submit to all registered
22 data brokers a “Delete My Data” request
23 that results in registered data brokers de-
24 leting all covered data related to such indi-
25 vidual that the data broker did not collect

1 directly from such individual or when act-
2 ing as a service provider.

3 (C) AFFORDABILITY.—A data broker may
4 not charge an individual a fee to exercise a
5 right under this paragraph.

6 (4) DO NOT COLLECT AND DELETE MY DATA
7 REQUESTS.—

8 (A) COMPLIANCE.—Subject to subpara-
9 graph (B), each data broker that receives a re-
10 quest from an individual using the mechanism
11 established under paragraph (3)(B)(iii) or para-
12 graph (3)(B)(iv), and not a third party on be-
13 half of the individual, shall comply with such
14 request not later than 30 days after the date on
15 which the request is received by the data
16 broker.

17 (B) EXCEPTION.—A data broker may de-
18 cline to fulfill a request from an individual, if—

19 (i) the data broker has actual knowl-
20 edge that the individual has been convicted
21 of a crime related to the abduction or sex-
22 ual exploitation of a child; and

23 (ii) the data collected by the data
24 broker is necessary—

1 (I) to carry out a national or
2 State-run sex offender registry; or
3 (II) for the National Center for
4 Missing and Exploited Children.

5 **SEC. 113. COMMISSION-APPROVED COMPLIANCE GUIDE-**
6 **LINES.**

7 (a) APPLICATION FOR COMPLIANCE GUIDELINE AP-
8 PROVAL.—

9 (1) IN GENERAL.—A covered entity or service
10 provider that is not a data broker and is not a large
11 data holder, or a group of such covered entities, may
12 apply to the Commission for approval of 1 or more
13 sets of compliance guidelines governing the collec-
14 tion, processing, retention, or transfer of covered
15 data by the covered entity or covered entities.

16 (2) APPLICATION REQUIREMENTS.—An applica-
17 tion under paragraph (1) shall include—

18 (A) a description of how the proposed
19 guidelines will meet or exceed the requirements
20 of this title;

21 (B) a description of the entities or activi-
22 ties the proposed guidelines are designed to
23 cover;

1 (C) a list of the covered entities, to the ex-
2 tent known at the time of application, that in-
3 tend to adhere to the proposed guidelines;

4 (D) a description of an independent orga-
5 nization, not associated with any of the in-
6 tended adhering covered entities, that will ad-
7 minister the proposed guidelines; and

8 (E) a description of how such intended ad-
9 hering entities will be assessed for adherence to
10 the proposed guidelines by the independent or-
11 ganization described in subparagraph (D).

12 (3) COMMISSION REVIEW.—

13 (A) INITIAL APPROVAL.—

14 (i) PUBLIC COMMENT PERIOD.—Not
15 later than 90 days after receipt of an ap-
16 plication regarding proposed guidelines
17 submitted pursuant to paragraph (1), the
18 Commission shall publish the application
19 and provide an opportunity for public com-
20 ment on such proposed guidelines.

21 (ii) APPROVAL CRITERIA.—The Com-
22 mission shall approve an application re-
23 garding proposed guidelines submitted pur-
24 suant to paragraph (1), including the inde-
25 pendent organization that will administer

1 the guidelines, if the applicant dem-
2 onstrates that the proposed guidelines—

3 (I) meet or exceed requirements
4 of this title;

5 (II) provide for regular review
6 and validation by an independent or-
7 ganization to ensure that the covered
8 entity or covered entities adhering to
9 the guidelines continue to meet or ex-
10 ceed the requirements of this title;
11 and

12 (III) include a means of enforce-
13 ment if a covered entity does not meet
14 or exceed the requirements in the
15 guidelines, which may include referral
16 to the Commission for enforcement
17 consistent with section 115 or referral
18 to the appropriate State attorney gen-
19 eral for enforcement consistent with
20 section 116.

21 (iii) **TIMELINE.**—Not later than 1
22 year after the date on which the Commis-
23 sion receives an application regarding pro-
24 posed guidelines pursuant to paragraph
25 (1), the Commission shall issue a deter-

1 mination approving or denying the applica-
2 tion, including the relevant independent or-
3 ganization, and providing the reasons for
4 approving or denying the application.

5 (B) APPROVAL OF MODIFICATIONS.—

6 (i) IN GENERAL.—If the independent
7 organization administering a set of guide-
8 lines approved under subparagraph (A)
9 makes significant changes to the guide-
10 lines, the independent organization shall
11 submit the updated guidelines to the Com-
12 mission for approval. As soon as feasible,
13 the Commission shall publish the updated
14 guidelines and provide an opportunity for
15 public comment.

16 (ii) TIMELINE.—The Commission
17 shall approve or deny any significant
18 change to guidelines submitted under
19 clause (i) not later than 180 days after the
20 date on which the Commission receives the
21 submission for approval.

22 (b) WITHDRAWAL OF APPROVAL.—

23 (1) IN GENERAL.—If at any time the Commis-
24 sion determines that guidelines previously approved
25 under this section no longer meet the requirements

1 of this title or that compliance with the approved
2 guidelines is insufficiently enforced by the inde-
3 pendent organization administering the guidelines,
4 the Commission shall notify the relevant covered en-
5 tity or group of covered entities and the independent
6 organization of the determination of the Commission
7 to withdraw approval of the guidelines, including the
8 basis for the determination.

9 (2) OPPORTUNITY TO CURE.—

10 (A) IN GENERAL.—Not later than 180
11 days after receipt of a notice under paragraph
12 (1), the covered entity or group of covered enti-
13 ties and the independent organization may cure
14 any alleged deficiency with the guidelines or the
15 enforcement of the guidelines and submit each
16 proposed cure to the Commission.

17 (B) EFFECT ON WITHDRAWAL OF AP-
18 PROVAL.—If the Commission determines that
19 cures proposed under subparagraph (A) elimi-
20 nate alleged deficiencies in the guidelines, the
21 Commission may not withdraw the approval of
22 such guidelines on the basis of such defi-
23 ciencies.

1 (c) CERTIFICATION.—A covered entity with guide-
2 lines approved by the Commission under this section
3 shall—

4 (1) publicly self-certify that the covered entity
5 is in compliance with the guidelines; and

6 (2) as part of the self-certification under para-
7 graph (1), indicate the independent organization re-
8 sponsible for assessing compliance with the guide-
9 lines.

10 (d) REBUTTABLE PRESUMPTION OF COMPLIANCE.—

11 A covered entity that is eligible to participate in guidelines
12 approved under this section, participates in the guidelines,
13 and is in compliance with the guidelines shall be entitled
14 to a rebuttable presumption that the covered entity is in
15 compliance with the relevant provisions of this title to
16 which the guidelines apply.

17 **SEC. 114. PRIVACY-ENHANCING TECHNOLOGY PILOT PRO-**
18 **GRAM.**

19 (a) PRIVACY-ENHANCING TECHNOLOGY DEFINED.—

20 In this section, the term “privacy-enhancing tech-
21 nology”—

22 (1) means any software or hardware solution,
23 cryptographic algorithm, or other technical process
24 of extracting the value of information without sub-

1 stantially reducing the privacy and security of the
2 information; and

3 (2) includes technologies with functionality
4 similar to homomorphic encryption, differential pri-
5 vacy, zero-knowledge proofs, synthetic data genera-
6 tion, federated learning, and secure multi-party com-
7 putation.

8 (b) ESTABLISHMENT.—Not later than 1 year after
9 the date of the enactment of this Act, the Commission
10 shall establish and carry out a pilot program to encourage
11 private sector use of privacy-enhancing technologies for
12 the purposes of protecting covered data to comply with
13 section 109.

14 (c) PURPOSES.—Under the pilot program established
15 under subsection (b), the Commission shall—

16 (1) develop and implement a petition process
17 for covered entities to request to be a part of the
18 pilot program; and

19 (2) build an auditing system that leverages pri-
20 vacy-enhancing technologies to support the enforce-
21 ment actions of the Commission.

22 (d) PETITION PROCESS.—A covered entity wishing to
23 be accepted into the pilot program established under sub-
24 section (b) shall demonstrate to the Commission that the
25 privacy-enhancing technologies to be used under the pilot

1 program by the covered entity will establish data security
2 practices that meet or exceed all or some of the require-
3 ments in section 109. If the covered entity demonstrates
4 the privacy-enhancing technologies meet or exceed the re-
5 quirements in section 109, the Commission may accept the
6 covered entity to be a part of the pilot program. If the
7 Commission does not accept a covered entity to be a part
8 of the pilot program, the Commission shall provide an ade-
9 quate response to the covered entity detailing why such
10 entity was not admitted to the pilot program. The covered
11 entity that was not admitted to the pilot program, may
12 subsequently revise their petition and amend any defi-
13 ciencies indicated by the Commission in their response to
14 the covered entity.

15 (e) REQUIREMENTS.—In carrying out the pilot pro-
16 gram established under subsection (b), the Commission
17 shall—

18 (1) receive input from private, public, and aca-
19 demic stakeholders; and

20 (2) develop ongoing public and private sector
21 engagement, in consultation with the Secretary of
22 Commerce, to disseminate voluntary, consensus-
23 based resources to increase the integration of pri-
24 vacy-enhancing technologies in data collection, shar-
25 ing, and analytics by the public and private sectors.

1 (f) CONCLUSION OF PILOT PROGRAM.—The Commis-
2 sion shall terminate the pilot program established under
3 subsection (b) not later than 10 years after the commence-
4 ment of the program.

5 (g) STUDY REQUIRED.—

6 (1) IN GENERAL.—The Comptroller General of
7 the United States shall conduct a study—

8 (A) to assess the progress of the pilot pro-
9 gram established under subsection (b);

10 (B) to determine the effectiveness of using
11 privacy-enhancing technologies at the Commis-
12 sion to support oversight of the data security
13 practices of covered entities; and

14 (C) to develop recommendations to improve
15 and advance privacy-enhancing technologies, in-
16 cluding by improving communication and co-
17 ordination between covered entities and the
18 Commission to increase implementation of pri-
19 vacy-enhancing technologies by such entities
20 and the Commission.

21 (2) INITIAL BRIEFING.—Not later than 3 years
22 after the date of the enactment of this Act, the
23 Comptroller General shall brief the Committee on
24 Energy and Commerce of the House of Representa-
25 tives and the Committee on Commerce, Science, and

1 Transportation of the Senate on the initial results of
2 the study conducted under paragraph (1).

3 (3) FINAL REPORT.—Not later than 240 days
4 after the date on which the briefing required by
5 paragraph (2) is conducted, the Comptroller General
6 shall submit to the Committee on Energy and Com-
7 merce of the House of Representatives and the Com-
8 mittee on Commerce, Science, and Transportation of
9 the Senate a final report setting forth the results of
10 the study conducted under paragraph (1), including
11 the recommendations developed under subparagraph
12 (C) of such paragraph.

13 (h) AUDIT OF COVERED ENTITIES.—The Commis-
14 sion shall, on an ongoing basis, audit covered entities who
15 have been accepted to be part of the pilot program estab-
16 lished under subsection (b) to determine whether such a
17 covered entity is maintaining the use and implementation
18 of privacy-enhancing technologies to secure covered data.

19 (i) WITHDRAWAL FROM THE PILOT PROGRAM.—If at
20 any time the Commission determines that a covered entity
21 accepted to be a part of the pilot program established
22 under subsection (b) is no longer maintaining the use of
23 privacy-enhancing technologies, the Commission shall no-
24 tify the covered entity of the determination of the Commis-
25 sion to withdraw approval for the covered entity to be a

1 part of the pilot program and the basis for doing so. Not
2 later than 180 days after the date on which a covered enti-
3 ty receives such notice, the covered entity may cure any
4 alleged deficiency with the use of privacy-enhancing tech-
5 nologies and submit each proposed cure to the Commis-
6 sion. If the Commission determines that such cures elimi-
7 nate alleged deficiencies with the use of privacy-enhancing
8 technologies, the Commission may not withdraw the ap-
9 proval of the covered entity to be a part of the pilot pro-
10 gram on the basis of such deficiencies.

11 (j) LIMITATIONS ON LIABILITY.—Any covered entity
12 that petitions, and is accepted, to be part of the pilot pro-
13 gram established under subsection (b), and actively imple-
14 ments and maintains the use of privacy-enhancing tech-
15 nologies, and is deemed to be in compliance with the pro-
16 gram shall—

17 (1) for any action under section 115 or 116 for
18 a violation of section 109, be deemed to be in com-
19 pliance with section 109 with respect to covered data
20 subject to the privacy-enhancing technologies; and

21 (2) for any action under section 117 for a viola-
22 tion of section 109, be entitled to a rebuttable pre-
23 sumption that such entity is in compliance with sec-
24 tion 109 with respect to the covered data subject to
25 the privacy-enhancing technologies.

1 **SEC. 115. ENFORCEMENT BY FEDERAL TRADE COMMIS-**
2 **SION.**

3 (a) NEW BUREAU.—

4 (1) IN GENERAL.—Subject to the availability of
5 appropriations, the Commission shall establish, with-
6 in the Commission, a new bureau comparable in
7 structure, size, organization, and authority to the ex-
8 isting bureaus within the Commission related to con-
9 sumer protection and competition.

10 (2) MISSION.—The mission of the bureau es-
11 tablished under this subsection shall be to assist the
12 Commission in exercising the authority of the Com-
13 mission under this title and related authorities.

14 (3) STAFF.—In staffing the bureau, the Com-
15 mission shall ensure it allocates full time employees
16 or full time employee equivalents including attor-
17 neys, economists, investigators, technologists, and
18 mental health professionals with experience in the
19 well-being of children and teens. For the purposes of
20 this paragraph, the term “technologists” means indi-
21 viduals with training and expertise including the
22 state of the art information technology, network or
23 data security, hardware or software development,
24 privacy-enhancing technologies, cryptography, com-
25 puter science, data science, advertising-technology,

1 web tracking, machine learning and other related
2 fields and applications.

3 (4) TIMELINE.—The bureau established under
4 this subsection shall be established, staffed, and fully
5 operational not later than 180 days after the date of
6 the enactment of this Act.

7 (b) ENFORCEMENT BY COMMISSION.—

8 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
9 TICES.—A violation of this title or a regulation pro-
10 mulgated under this title shall be treated as a viola-
11 tion of a rule defining an unfair or deceptive act or
12 practice prescribed under section 18(a)(1)(B) of the
13 Federal Trade Commission Act (15 U.S.C.
14 57a(a)(1)(B)).

15 (2) POWERS OF COMMISSION.—

16 (A) IN GENERAL.—Except as provided in
17 paragraph (3) or otherwise provided in this
18 title, the Commission shall enforce this title and
19 the regulations promulgated under this title in
20 the same manner, by the same means, and with
21 the same jurisdiction, powers, and duties as
22 though all applicable terms and provisions of
23 the Federal Trade Commission Act (15 U.S.C.
24 41 et seq.) were incorporated into and made a
25 part of this title.

1 (B) PRIVILEGES AND IMMUNITIES.—Any
2 entity that violates this title or a regulation
3 promulgated under this title shall be subject to
4 the penalties and entitled to the privileges and
5 immunities provided in the Federal Trade Com-
6 mission Act (15 U.S.C. 41 et seq.).

7 (3) COMMON CARRIERS AND NONPROFITS.—
8 Notwithstanding section 4, 5(a)(2), or 6 of the Fed-
9 eral Trade Commission Act (15 U.S.C. 44; 45(a)(2);
10 46) or any jurisdictional limitation of the Commis-
11 sion, the Commission shall also enforce this title,
12 and the regulations promulgated under this title, in
13 the same manner provided in paragraphs (1) and (2)
14 of this subsection with respect to—

15 (A) common carriers subject to title II of
16 the Communications Act of 1934 (47 U.S.C.
17 201 et seq.); and

18 (B) organizations not organized to carry
19 on business for their own profit or that of their
20 members.

21 (4) PENALTY OFFSET FOR STATE OR INDI-
22 VIDUAL ACTIONS.—Any amount that a court orders
23 an entity to pay in an action under this subsection
24 shall be offset by any amount a court has ordered
25 the entity to pay in an action brought against the

1 entity for the same violation under section 116 or
2 117.

3 (5) PRIVACY AND SECURITY VICTIMS RELIEF
4 FUND.—

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

11 (B) DEPOSITS.—The Commission or the
12 Attorney General of the United States, as appli-
13 cable, shall deposit into the Victims Relief Fund
14 the amount of any civil penalty obtained in any
15 civil action the Commission, or the Attorney
16 General on behalf of the Commission, com-
17 mences to enforce this title or a regulation pro-
18 mulgated under this title.

19 (C) USE OF FUND AMOUNTS.—

20 (i) AVAILABILITY TO THE COMMIS-
21 SION.—Notwithstanding section 3302 of
22 title 31, United States Code, amounts in
23 the Victims Relief Fund shall be available
24 to the Commission, without fiscal year lim-
25 itation, to provide redress, damages, pay-

1 ments or compensation, or other monetary
2 relief to persons affected by an act or prac-
3 tice for which civil penalties, other mone-
4 tary relief, or any other forms of relief (in-
5 cluding injunctive relief) have been ordered
6 in a civil action or administrative pro-
7 ceeding the Commission commences, or in
8 any civil action the Attorney General of the
9 United States commences on behalf of the
10 Commission, to enforce this title or a regu-
11 lation promulgated under this title.

12 (ii) OTHER PERMISSIBLE USES.—To
13 the extent that individuals cannot be lo-
14 cated or such redress, payments or com-
15 pensation, or other monetary relief are oth-
16 erwise not practicable, the Commission
17 may use amounts in the Victims Relief
18 Fund for the purpose of—

19 (I) consumer or business edu-
20 cation relating to data privacy or data
21 security; or

22 (II) engaging in technological re-
23 search that the Commission considers
24 necessary to implement this title, in-
25 cluding promoting privacy-enhancing

1 technologies that promote compliance
2 with this title.

3 (D) CALCULATION.—Any amount that the
4 Commission provides to a person as redress,
5 payments or compensation, or other monetary
6 relief under subparagraph (C) with respect to a
7 violation by an entity shall be offset by any
8 amount the person received from an action
9 brought against the entity for the same viola-
10 tion under section 116 or 117.

11 (E) RULE OF CONSTRUCTION.—Amounts
12 collected and deposited in the Victims Relief
13 Fund may not be construed to be Government
14 funds or appropriated monies and may not be
15 subject to apportionment for the purpose of
16 chapter 15 of title 31, United States Code, or
17 under any other authority.

18 (c) REPORT.—

19 (1) IN GENERAL.—Not later than 4 years after
20 the date of the enactment of this Act, and annually
21 thereafter, the Commission shall submit to Congress
22 a report describing investigations conducted during
23 the prior year with respect to violations of this title,
24 including—

1 (A) the number of such investigations the
2 Commission commenced;

3 (B) the number of such investigations the
4 Commission closed with no official agency ac-
5 tion;

6 (C) the disposition of such investigations,
7 if such investigations have concluded and re-
8 sulted in official agency action; and

9 (D) for each investigation that was closed
10 with no official agency action, the industry sec-
11 tors of the covered entities subject to each in-
12 vestigation.

13 (2) PRIVACY PROTECTIONS.—A report required
14 under paragraph (1) may not include the identity of
15 any person who is the subject of an investigation or
16 any other information that identifies such a person.

17 (3) ANNUAL PLAN.—Not later than 540 days
18 after the date of the enactment of this Act, and an-
19 nually thereafter, the Commission shall submit to
20 Congress a plan for the next calendar year describ-
21 ing the projected activities of the Commission under
22 this title, including—

23 (A) the policy priorities of the Commission
24 and any changes to the previous policy prior-
25 ities of the Commission;

1 (B) any rulemaking proceedings projected
2 to be commenced, including any such pro-
3 ceedings to amend or repeal a rule;

4 (C) any plans to develop, update, or with-
5 draw guidelines or guidance required under this
6 title;

7 (D) any plans to restructure the Commis-
8 sion; and

9 (E) projected dates and timelines, or
10 changes to projected dates and timelines, asso-
11 ciated with any of the requirements under this
12 title.

13 **SEC. 116. ENFORCEMENT BY STATES.**

14 (a) CIVIL ACTION.—

15 (1) IN GENERAL.—In any case in which the at-
16 torney general of a State, the chief consumer protec-
17 tion officer of a State, or an officer or office of a
18 State authorized to enforce privacy or data security
19 laws applicable to covered entities or service pro-
20 viders has reason to believe that an interest of the
21 residents of the State has been or is adversely af-
22 fected by the engagement of any entity in an act or
23 practice that violates this title or a regulation pro-
24 mulgated under this title, the attorney general, chief
25 consumer protection officer, or other authorized offi-

1 cer or office of the State may bring a civil action in
2 the name of the State, or as *parens patriae* on be-
3 half of the residents of the State, in an appropriate
4 Federal district court of the United States to—

5 (A) enjoin such act or practice;

6 (B) enforce compliance with this title or
7 the regulations promulgated under this title;

8 (C) obtain civil penalties;

9 (D) obtain damages, restitution, or other
10 compensation on behalf of the residents of the
11 State;

12 (E) obtain reasonable attorney's fees and
13 other litigation costs reasonably incurred; or

14 (F) obtain such other relief as the court
15 may consider to be appropriate.

16 (2) LIMITATION.—In any case with respect to
17 which the attorney general of a State, the chief con-
18 sumer protection officer of a State, or an officer or
19 office of a State authorized to enforce privacy or
20 data security laws applicable to covered entities or
21 service providers brings an action under paragraph
22 (1), no other officer or office of the same State may
23 institute a civil action under paragraph (1) against
24 the same defendant for the same violation of this
25 title or regulation promulgated under this title.

1 (b) RIGHTS OF THE COMMISSION.—

2 (1) IN GENERAL.—Except if not feasible, a
3 State officer shall notify the Commission in writing
4 prior to initiating a civil action under subsection (a).
5 Such notice shall include a copy of the complaint to
6 be filed to initiate such action. Upon receiving such
7 notice, the Commission may intervene in such action
8 and, upon intervening—

9 (A) be heard on all matters arising in such
10 action; and

11 (B) file petitions for appeal of a decision in
12 such action.

13 (2) NOTIFICATION TIMELINE.—If not feasible
14 for a State officer to provide the notification re-
15 quired by paragraph (1) before initiating a civil ac-
16 tion under subsection (a), the State officer shall no-
17 tify the Commission immediately after initiating the
18 civil action.

19 (c) ACTIONS BY THE COMMISSION.—In any case in
20 which a civil action is instituted by or on behalf of the
21 Commission for a violation of this title or a regulation pro-
22 mulgated under this title, no attorney general of a State,
23 chief consumer protection officer of a State, or officer or
24 office of a State authorized to enforce privacy or data se-
25 curity laws may, during the pendency of such action, insti-

1 tute a civil action against any defendant named in the
2 complaint in the action instituted by or on behalf of the
3 Commission for a violation of this title or a regulation pro-
4 mulgated under this title that is alleged in such complaint.

5 (d) INVESTIGATORY POWERS.—Nothing in this title
6 may be construed to prevent the attorney general of a
7 State, the chief consumer protection officer of a State, or
8 an officer or office of a State authorized to enforce privacy
9 or data security laws applicable to covered entities or serv-
10 ice providers from exercising the powers conferred on such
11 officer or office to conduct investigations, to administer
12 oaths or affirmations, or to compel the attendance of wit-
13 nesses or the production of documentary or other evidence.

14 (e) VENUE; SERVICE OF PROCESS.—

15 (1) VENUE.—Any action brought under sub-
16 section (a) may be brought in any Federal district
17 court of the United States that meets applicable re-
18 quirements relating to venue under section 1391 of
19 title 28, United States Code.

20 (2) SERVICE OF PROCESS.—In an action
21 brought under subsection (a), process may be served
22 in any district in which the defendant—

23 (A) is an inhabitant; or

24 (B) may be found.

1 (f) GAO STUDY.—Not later than 1 year after the
2 date of the enactment of this Act, the Comptroller General
3 of the United States shall conduct a study of the practice
4 of State attorneys general hiring, or otherwise contracting
5 with, outside firms to assist in enforcement efforts pursu-
6 ant to this title, which shall include the study of—

7 (1) the frequency with which each State attor-
8 ney general hires or contracts with outside firms to
9 assist in such enforcement efforts;

10 (2) the contingency fees, hourly rates, and
11 other costs of hiring or contracting with outside
12 firms;

13 (3) the types of matters for which outside firms
14 are hired or contracted;

15 (4) the bid and selection process for such out-
16 side firms, including reviews of conflicts of interest;

17 (5) the practices State attorneys general set in
18 place to protect sensitive information that would be-
19 come accessible by outside firms while the outside
20 firms are assisting in such enforcement efforts;

21 (6) the percentage of monetary recovery that is
22 returned to victims and the percentage of such re-
23 covery that is retained by outside firms; and

24 (7) the market average for the hourly rate of
25 hired or contracted attorneys in each market.

1 (g) PRESERVATION OF STATE POWERS.—Except as
2 provided in subsections (a)(2) and (c), no provision of this
3 section may be construed as altering, limiting, or affecting
4 the authority of a State attorney general, the chief con-
5 sumer protection officer of a State, or an officer or office
6 of a State authorized to enforce laws applicable to covered
7 entities or service providers to—

8 (1) bring an action or other regulatory pro-
9 ceeding arising solely under the laws in effect in
10 such State; or

11 (2) exercise the powers conferred on the attor-
12 ney general, chief consumer protection officer, or of-
13 ficer or office by the laws of such State, including
14 the ability to conduct investigations, to administer
15 oaths or affirmations, or to compel the attendance of
16 witnesses or the production of documentary or other
17 evidence.

18 (h) CALCULATION.—Any amount that a court orders
19 an entity to pay to a person under this section shall be
20 offset by any amount the person received from an action
21 brought against the entity for the same violation under
22 section 115 or 117.

23 **SEC. 117. ENFORCEMENT BY PERSONS.**

24 (a) CIVIL ACTION.—

1 (1) IN GENERAL.—Subject to subsections (b)
2 and (c), a person may bring a civil action against a
3 covered entity or service provider for a violation of
4 subsection (b) or (c) of section 102, subsection (a)
5 or (e) of section 104, section 105, subsection (a) or
6 (b)(2) of section 106, section 107, section 108, sec-
7 tion 109 to the extent such claim alleges a data
8 breach arising from a violation of subsection (a) of
9 such section, subsection (d) of section 111, or sub-
10 section (c)(4) of section 112, or a regulation promul-
11 gated thereunder, in an appropriate Federal district
12 court of the United States.

13 (2) RELIEF.—

14 (A) IN GENERAL.—In a civil action
15 brought under paragraph (1) in which the
16 plaintiff prevails, the court may award the
17 plaintiff—

18 (i) an amount equal to the sum of any
19 actual damages;

20 (ii) injunctive relief, including an
21 order that the entity retrieve any covered
22 data transferred in violation of this title;

23 (iii) declaratory relief; and

24 (iv) reasonable attorney fees and liti-
25 gation costs.

1 (B) BIOMETRIC AND GENETIC INFORMA-
2 TION.—In a civil action brought under para-
3 graph (1) for a violation of this title with re-
4 spect to section 102(c), in which the plaintiff
5 prevails, if the conduct underlying the violation
6 occurred primarily and substantially in Illinois,
7 the court may award the plaintiff—

8 (i) for a violation involving biometric
9 information, the same relief as set forth in
10 section 20 of the Biometric Information
11 Privacy Act (740 ILCS 14/20), as such
12 statute read on December 31, 2024; or

13 (ii) for a violation involving genetic in-
14 formation, the same relief as set forth in
15 section 40 of the Genetic Information Pri-
16 vacy Act (410 ILCS 513/40), as such stat-
17 ute read on December 31, 2024.

18 (C) DATA SECURITY.—

19 (i) IN GENERAL.—In a civil action
20 brought under paragraph (1) for a viola-
21 tion of this title alleging unauthorized ac-
22 cess of covered information as a result of
23 a violation of section 109(a), in which the
24 plaintiff prevails, the court may award a
25 plaintiff who is a resident of California the

1 same relief as set forth in section
2 1798.150 of the California Civil Code, as
3 such statute read on January 1, 2024.

4 (ii) COVERED INFORMATION DE-
5 FINED.—For purposes of this subpara-
6 graph, the term “covered information”
7 means the following:

8 (I) A username, email address, or
9 telephone number of an individual in
10 combination with a password or secu-
11 rity question or answer that would
12 permit access to an account held by
13 the individual that contains or pro-
14 vides access to sensitive covered data.

15 (II) The first name or first initial
16 of an individual and the last name of
17 the individual in combination with 1
18 or more of the following categories of
19 sensitive covered data, if either the
20 name or the sensitive covered data are
21 not encrypted or redacted:

22 (aa) A government-issued
23 identifier described in section
24 101(49)(A)(i).

1 (bb) A financial account
2 number described in section
3 101(49)(A)(iv).

4 (cc) Health information, but
5 only to the extent such informa-
6 tion reveals the history of med-
7 ical treatment or diagnosis by a
8 health care professional of the in-
9 dividual.

10 (dd) Biometric information.

11 (ee) Genetic information.

12 (D) LIMITATIONS ON DUAL ACTIONS.—

13 Any amount that a court orders an entity to
14 pay to a person under subparagraph (A)(i),
15 (B), or (C) shall be offset by any amount the
16 person received from an action brought against
17 the entity for the same violation under section
18 115 or 116.

19 (b) OPPORTUNITY TO CURE IN ACTIONS FOR IN-
20 JUNCTIVE RELIEF.—

21 (1) NOTICE.—Subject to paragraph (3), an ac-
22 tion for injunctive relief may be brought by a person
23 under this section only if, prior to initiating such ac-
24 tion against an entity for injunctive relief, the per-
25 son provides to the entity 30 days written notice

1 identifying the specific provisions of this title the
2 person alleges have been or are being violated.

3 (2) EFFECT OF CURE.—In the event a cure is
4 possible, if within the 60 days the entity cures the
5 noticed violation and provides the person an express
6 written statement that the violation has been cured
7 and that no further such violations shall occur, an
8 action for injunctive relief may not be permitted
9 with respect to the noticed violation.

10 (3) INJUNCTIVE RELIEF FOR A SUBSTANTIAL
11 PRIVACY HARM.—Notice is not required under para-
12 graph (1) prior to bringing an action for injunctive
13 relief for a violation that resulted in a substantial
14 privacy harm.

15 (c) NOTICE OF ACTIONS SEEKING ACTUAL DAM-
16 AGES.—

17 (1) NOTICE.—An action under this section for
18 actual damages may be brought by a person only if,
19 prior to initiating such action against an entity, the
20 person provides the entity 60 days written notice
21 identifying the specific provisions of this title the
22 person alleges have been or are being violated.

23 (2) SETTLEMENT.—A covered entity who re-
24 ceives a written notice from a person under para-

1 graph (1) of this subsection may settle with the per-
2 son who sent the written notice.

3 (3) EFFECT OF SETTLEMENT.—In the event of
4 a settlement, the terms of such settlement shall gov-
5 ern future action for actual damages between the
6 parties to the settlement, related to the underlying
7 facts that resulted in the settlement.

8 (4) NO NOTICE REQUIRED FOR A SUBSTANTIAL
9 PRIVACY HARM.—Notice is not required under para-
10 graph (1) prior to bringing an action for actual
11 damages for a violation of this title that resulted in
12 a substantial privacy harm, if such action includes a
13 claim for a preliminary injunction or temporary re-
14 straining order.

15 (d) PRE-DISPUTE ARBITRATION AGREEMENTS.—

16 (1) IN GENERAL.—Notwithstanding any other
17 provision of law, at the election of the person alleg-
18 ing a violation of this title, no pre-dispute arbitra-
19 tion agreement shall be valid or enforceable with re-
20 spect to—

21 (A) a claim alleging a violation involving
22 an individual under the age of 18; or

23 (B) a claim alleging a violation that re-
24 sulted in a substantial privacy harm.

1 (2) DETERMINATION OF APPLICABILITY.—Any
2 issue as to whether this subsection applies to a dis-
3 pute shall be determined under Federal law. The ap-
4 plicability of this subsection to an agreement to arbi-
5 trate and the validity and enforceability of an agree-
6 ment to which this subsection applies shall be deter-
7 mined by a Federal court, rather than an arbitrator,
8 irrespective of whether the party resisting arbitra-
9 tion challenges the arbitration agreement specifically
10 or in conjunction with other terms of the contract
11 containing the agreement, and irrespective of wheth-
12 er the agreement purports to delegate the deter-
13 mination to an arbitrator.

14 (3) PRE-DISPUTE ARBITRATION AGREEMENT
15 DEFINED.—For purposes of this subsection, the
16 term “pre-dispute arbitration agreement” means any
17 agreement to arbitrate a dispute that has not arisen
18 at the time of the making of the agreement.

19 (e) COMBINED NOTICES.—A person may combine the
20 notices required by subsections (b)(1) and (c)(1) into a
21 single notice, if the single notice complies with the require-
22 ments of each such subsection.

23 (f) BAD FAITH.—If a person represented by counsel
24 brings a civil action against a covered entity or service
25 provider requesting actual damages from that covered en-

1 tity or service provider regarding a specific claim described
2 in a claim, and fails to provide notice to such covered enti-
3 ty or service provider when required to do so in this sec-
4 tion, the action may be dismissed without prejudice and
5 may not be reinstated until such person has complied with
6 the notice requirements in this section.

7 **SEC. 118. RELATION TO OTHER LAWS.**

8 (a) **PREEMPTION OF STATE LAWS.**—

9 (1) **CONGRESSIONAL INTENT.**—The purposes of
10 this section are to—

11 (A) establish a uniform national privacy
12 and data security standard in the United States
13 to prevent administrative costs and burdens
14 from being placed on interstate commerce; and

15 (B) expressly preempt the laws of a State
16 or political subdivision of a State as provided in
17 this subsection.

18 (2) **PREEMPTION.**—Except as provided in para-
19 graph (3), no State or political subdivision of a
20 State may adopt, maintain, enforce, impose, or con-
21 tinue in effect any law, regulation, rule, requirement,
22 prohibition, standard, or other provision covered by
23 the provisions of this title or a rule, regulation, or
24 requirement promulgated under this title.

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

5 (A) Consumer protection laws of general
6 applicability, such as laws regulating deceptive,
7 unfair, or unconscionable practices.

8 (B) Civil rights laws.

9 (C) Provisions of laws that address the pri-
10 vacy rights or other protections of employees or
11 employee information.

12 (D) Provisions of laws that address the
13 privacy rights or other protections of students
14 or student information.

15 (E) Provisions of laws, insofar as such pro-
16 visions address notification requirements in the
17 event of a data breach.

18 (F) Contract or tort law.

19 (G) Criminal laws.

20 (H) Civil laws regarding—

21 (i) blackmail;

22 (ii) stalking (including cyberstalking);

23 (iii) cyberbullying;

1 (iv) intimate images (whether authen-
2 tic or computer-generated) known to be
3 nonconsensual;

4 (v) child abuse;

5 (vi) child sexual abuse material;

6 (vii) child abduction or attempted
7 child abduction;

8 (viii) child trafficking; or

9 (ix) sexual harassment.

10 (I) Public safety or sector-specific laws un-
11 related to privacy or data security, but only to
12 the extent such laws do not directly conflict
13 with the provisions of this title.

14 (J) Provisions of laws that address public
15 records, criminal justice information systems,
16 arrest records, mug shots, conviction records, or
17 non-conviction records.

18 (K) Provisions of laws that address bank-
19 ing records, financial records, tax records, So-
20 cial Security numbers, credit cards, identity
21 theft, credit reporting and investigations, credit
22 repair, credit clinics, or check-cashing services.

23 (L) Provisions of laws that address elec-
24 tronic surveillance, wiretapping, or telephone
25 monitoring.

1 (M) Provisions of laws that address unso-
2 licited email messages, telephone solicitation, or
3 caller identification.

4 (N) Provisions of laws that protect the pri-
5 vacy of health information, healthcare informa-
6 tion, medical information, medical records, HIV
7 status, or HIV testing.

8 (O) Provisions of laws that address the
9 confidentiality of library records.

10 (P) Provisions of laws that address the use
11 of encryption as a means of providing data se-
12 curity.

13 (4) PREEMPTION LIMITATIONS.—Notwith-
14 standing paragraph (2), the provisions of this title
15 shall preempt any State law, rule, or regulation that
16 provides protections for children or teens only to the
17 extent that such State law, rule, or regulation con-
18 flicts with a provision of this title. Nothing in this
19 title shall be construed to prohibit any State from
20 enacting a law, rule, or regulation that provides
21 greater protection to children or teens than the pro-
22 visions of this title.

23 (b) FEDERAL LAW PRESERVATION.—

1 (1) IN GENERAL.—Nothing in this title or a
2 regulation promulgated under this title may be con-
3 strued to limit—

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

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

12 (C) any other provision of Federal law, ex-
13 cept as otherwise provided in this title.

14 (2) ANTITRUST SAVINGS CLAUSE.—

15 (A) ANTITRUST LAWS DEFINED.—For pur-
16 poses of this paragraph, the term “antitrust
17 laws”—

18 (i) has the meaning given such term
19 in subsection (a) of the first section of the
20 Clayton Act (15 U.S.C. 12(a)); and

21 (ii) includes section 5 of the Federal
22 Trade Commission Act (15 U.S.C. 45), to
23 the extent such section applies to unfair
24 methods of competition.

1 (B) FULL APPLICATION OF THE ANTI-
2 TRUST LAWS.—Nothing in this title or a regula-
3 tion promulgated under this title may be con-
4 strued to modify, impair, supersede the oper-
5 ation of, or preclude the application of the anti-
6 trust laws.

7 (3) APPLICATION OF OTHER FEDERAL PRIVACY
8 REQUIREMENTS.—

9 (A) IN GENERAL.—To the extent that a
10 covered entity or service provider is required to
11 comply with any of the laws and regulations de-
12 scribed in subparagraph (B), such covered enti-
13 ty or service provider is not subject to this title
14 with respect to the activities governed by the re-
15 quirements of such laws and regulations.

16 (B) LAWS AND REGULATIONS DE-
17 SCRIBED.—The laws and regulations described
18 in this subparagraph include the following:

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

21 (ii) Part C of title XI of the Social
22 Security Act (42 U.S.C. 1320d et seq.).

23 (iii) Subtitle D of the Health Informa-
24 tion Technology for Economic and Clinical
25 Health Act (42 U.S.C. 17921 et seq.).

1 (iv) The regulations promulgated pur-
2 suant to section 264(c) of the Health In-
3 surance Portability and Accountability Act
4 of 1996 (42 U.S.C. 1320d–2 note).

5 (v) The requirements regarding the
6 confidentiality of substance use disorder
7 information under section 543 of the Pub-
8 lic Health Service Act (42 U.S.C. 290dd–
9 2) or any regulation promulgated under
10 such section.

11 (vi) The Fair Credit Reporting Act
12 (15 U.S.C. 1681 et seq.).

13 (vii) Section 444 of the General Edu-
14 cation Provisions Act (commonly known as
15 the “Family Educational Rights and Pri-
16 vacy Act of 1974”) (20 U.S.C. 1232g) and
17 part 99 of title 34, Code of Federal Regu-
18 lations (or any successor regulation), to
19 the extent a covered entity or service pro-
20 vider is an educational agency or institu-
21 tion (as defined in such section or section
22 99.3 of title 34, Code of Federal Regula-
23 tions (or any successor regulation)).

24 (viii) The regulations related to the
25 protection of human subjects under part

1 46 of title 45, Code of Federal Regula-
2 tions.

3 (ix) Regulations and agreements re-
4 lated to information collected as part of
5 human subjects research pursuant to the
6 good clinical practice guidelines issued by
7 The International Council for
8 Harmonisation of Technical Requirements
9 for Pharmaceuticals for Human Use; the
10 protection of human subjects under 21
11 C.F.R. Parts 6, 50, and 56, or personal
12 data used or shared in research conducted
13 in accordance with the requirements set
14 forth in this chapter, or other research
15 conducted in accordance with applicable
16 law.

17 (x) The Federal Health Care Quality
18 Improvement Act of 1986 (42 U.S.C.
19 11101 et seq.).

20 (xi) The Federal Patient Safety and
21 Quality Improvement Act (42 U.S.C. 299b-
22 21 et seq.).

23 (xii) The Drivers Privacy Protection
24 Act.

1 (C) IMPLEMENTATION GUIDANCE.—Not
2 later than 1 year after the date of the enact-
3 ment of this Act, the Commission shall issue
4 guidance with respect to the implementation of
5 this paragraph.

6 (4) APPLICATION OF OTHER FEDERAL DATA
7 SECURITY REQUIREMENTS.—

8 (A) IN GENERAL.—To the extent that a
9 covered entity or service provider is required to
10 comply with any of the laws and regulations de-
11 scribed in subparagraph (B), such covered enti-
12 ty or service provider is not subject to this title
13 with respect to the activities governed by the re-
14 quirements of such laws and regulations.

15 (B) LAWS AND REGULATIONS DE-
16 SCRIBED.—The laws and regulations described
17 in this subparagraph include the following:

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

20 (ii) Subtitle D of the Health Informa-
21 tion Technology for Economic and Clinical
22 Health Act (42 U.S.C. 17921 et seq.).

23 (iii) Part C of title XI of the Social
24 Security Act (42 U.S.C. 1320d et seq.).

1 (iv) The regulations promulgated pur-
2 suant to section 264(c) of the Health In-
3 surance Portability and Accountability Act
4 of 1996 (42 U.S.C. 1320d–2 note).

5 (v) The requirements regarding the
6 confidentiality of substance use disorder
7 information under section 543 of the Pub-
8 lic Health Service Act (42 U.S.C. 290dd–
9 2) or any regulation promulgated under
10 such section.

11 (vi) The Fair Credit Reporting Act
12 (15 U.S.C. 1681 et seq.).

13 (vii) Section 444 of the General Edu-
14 cation Provisions Act (commonly known as
15 the “Family Educational Rights and Pri-
16 vacy Act of 1974”) (20 U.S.C. 1232g) and
17 part 99 of title 34, Code of Federal Regu-
18 lations (or any successor regulation), to
19 the extent a covered entity or service pro-
20 vider is an educational agency or institu-
21 tion (as defined in such section or section
22 99.3 of title 34, Code of Federal Regula-
23 tions (or any successor regulation)).

24 (viii) The regulations related to the
25 protection of human subjects under part

1 46 of title 45, Code of Federal Regula-
2 tions.

3 (ix) Regulations and agreements re-
4 lated to information collected as part of
5 human subjects research pursuant to the
6 good clinical practice guidelines issued by
7 The International Council for
8 Harmonisation of Technical Requirements
9 for Pharmaceuticals for Human Use; the
10 protection of human subjects under 21
11 C.F.R. Parts 6, 50, and 56, or personal
12 data used or shared in research conducted
13 in accordance with the requirements set
14 forth in this chapter, or other research
15 conducted in accordance with applicable
16 law.

17 (x) The Federal Health Care Quality
18 Improvement Act of 1986 (42 U.S.C.
19 11101 et seq.).

20 (xi) The Federal Patient Safety and
21 Quality Improvement Act (42 U.S.C. 299b-
22 21 et seq.).

23 (xii) The Drivers Privacy Protection
24 Act.

1 (C) IMPLEMENTATION GUIDANCE.—Not
2 later than 1 year after the date of the enact-
3 ment of this Act, the Commission shall issue
4 guidance with respect to the implementation of
5 this paragraph.

6 (c) PRESERVATION OF COMMON LAW OR STATUTORY
7 CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this
8 title, nor any amendment, standard, rule, requirement, as-
9 sessment, law, or regulation promulgated under this title,
10 may be construed to preempt, displace, or supplant any
11 Federal or State common law rights or remedies, or any
12 statute creating a remedy for civil relief, including any
13 cause of action for personal injury, wrongful death, prop-
14 erty damage, or other financial, physical, reputational, or
15 psychological injury based in negligence, strict liability,
16 products liability, failure to warn, an objectively offensive
17 intrusion into the private affairs or concerns of an indi-
18 vidual, or any other legal theory of liability under any Fed-
19 eral or State common law, or any State statutory law, ex-
20 cept that the fact of a violation of this title or a regulation
21 promulgated under this title may not be pleaded as an
22 element of any violation of such law.

23 (d) NONAPPLICATION OF CERTAIN PROVISIONS OF
24 THE COMMUNICATIONS ACT OF 1934 AND TELECOMMUNI-

1 COMMUNICATIONS ACT OF 1996 AS IT RELATES TO FCC PRIVACY
2 AND DATA SECURITY LAWS AND REGULATIONS.—

3 (1) IN GENERAL.—Except as provided in para-
4 graph (2), sections 201, 202, 222, 338(i), and 631
5 of the Communications Act of 1934, as amended,
6 and section 706 of the Telecommunications Act of
7 1996, as amended (47 U.S.C. 201, 202, 222, 338(i),
8 551, 1302), and any regulation or orders promul-
9 gated by the Federal Communications Commission
10 under any such section, does not apply to any cov-
11 ered entity or service provider with respect to the
12 collection, processing, retention, transfer, or security
13 of covered data or its equivalent, to the extent that
14 those provisions of the Communications Act or any
15 regulations or orders adopted pursuant to those pro-
16 visions of the Communications Act would otherwise
17 govern the collection, processing, retention, transfer,
18 or security of covered data or its equivalent in order
19 to protect consumer privacy or the security of such
20 data and instead shall be governed by the require-
21 ments of this Act.

22 (2) EXCEPTIONS.—Paragraph (1) does not su-
23 perseede any authority of the Federal Communica-
24 tions Commission with respect to the following:

1 (A) Any emergency services, as defined in
2 section 7 of the Wireless Communications and
3 Public Safety Act of 1999 (47 U.S.C. 615b).

4 (B) Proceedings to implement section 227
5 of the Communications Act (47 U.S.C. 227) or
6 the Telephone Robocall Abuse Criminal En-
7 forcement and Deterrence Act of 2019 (Public
8 Law 116–105; 133 Stat. 3274), or any other
9 authority used by the Federal Communications
10 Commission to prevent or reduce unwanted tele-
11 phone calls or text messages.

12 (C) An enforcement action alleging or find-
13 ing a violation of a provision of the Commu-
14 nications Act specified in paragraph (1), where
15 such action was adopted by the Federal Com-
16 munications Commission prior to the date of
17 the enactment of this Act.

18 (D) Subsection (a) of section 222 of the
19 Communications Act to the extent it imposes a
20 duty on every telecommunications carrier to
21 protect the confidentiality of proprietary infor-
22 mation of, and relating to, other telecommuni-
23 cations carriers and equipment manufacturers.

1 (E) Subsections (b), (d), and (g) of section
2 222 of the Communications Act of 1934 (47
3 U.S.C. 222).

4 (F) Any obligation of an international
5 treaty related to the exchange of traffic imple-
6 mented and enforced by the Federal Commu-
7 nications Commission.

8 **SEC. 119. CHILDREN'S ONLINE PRIVACY PROTECTION ACT**
9 **OF 1998.**

10 Nothing in this title may be construed to relieve or
11 change any obligation that a covered entity or other per-
12 son may have under the Children's Online Privacy Protec-
13 tion Act of 1998 (15 U.S.C. 6501 et seq.).

14 **SEC. 120. DATA PROTECTIONS FOR COVERED MINORS.**

15 (a) PROHIBITION ON FIRST-PARTY AND TARGETED
16 ADVERTISING TO COVERED MINORS.—A covered entity or
17 service provider acting on behalf of a covered entity may
18 not engage in targeted advertising or first-party adver-
19 tising to an individual if the covered entity has knowledge
20 that the individual is a covered minor, except that a cov-
21 ered entity or service provider may present or display to
22 a covered minor age-appropriate advertisements intended
23 for an audience of covered minors, so long as the covered
24 entity or service provider acting on behalf of a covered
25 entity does not use any covered data other than whether

1 the individual that receives the advertisement is a covered
2 minor or the device that receives the advertisement is
3 linked or reasonably linkable to one or more individuals,
4 at least one of whom is a covered minor.

5 (b) DATA TRANSFER REQUIREMENTS RELATED TO
6 CHILDREN AND TEENS.—

7 (1) IN GENERAL.—Notwithstanding section
8 102(b), a covered entity or an entity acting as a
9 service provider may not transfer or direct a service
10 provider to transfer the covered data of a covered
11 minor to a third party if the covered entity—

12 (A) has knowledge that the individual is a
13 covered minor; and

14 (B) has not obtained affirmative express
15 consent unless the transfer is necessary, propor-
16 tionate, and limited to a purpose expressly per-
17 mitted by paragraph (2), (3), (4), (8), (9), (11),
18 (12), or (13) of section 102(d).

19 (2) EXCEPTION.—A covered entity or service
20 provider may collect, process, retain, or transfer cov-
21 ered data of an individual that the covered entity or
22 service provider knows is under the age of 18 solely
23 in order to submit information relating to child vic-
24 timization to law enforcement or to the nonprofit,
25 national resource center and clearinghouse congres-

1 sionally designated to provide assistance to victims,
2 families, child-serving professionals, and the general
3 public on missing and exploited children issues.

4 (c) IN GENERAL.—The Commission may conduct a
5 rulemaking pursuant to section 553 of title 5, United
6 States Code, to establish processes for parents and teens
7 to exercise the rights provided to them in this title with
8 respect to covered entities and data brokers. Any such
9 rulemaking should take into account the specific needs of
10 parents, children, and teens and should consider how best
11 to harmonize the processes provided for under this title
12 with the processes and guidance provided for under title
13 II and by the Children’s Online Privacy Protection Act
14 of 1998 (15 U.S.C. 6501 et. seq) and any rulemakings
15 undertaken by the Commission thereunder. It should also
16 consider options for reducing undue burdens on parents,
17 children, teens, covered entities and data brokers.

18 **SEC. 121. TERMINATION OF FTC RULEMAKING ON COM-**
19 **MERCIAL SURVEILLANCE AND DATA SECU-**
20 **RITY.**

21 Beginning on the date of the enactment of this Act,
22 the rulemaking proposed in the advance notice of proposed
23 rulemaking titled “Trade Regulation Rule on Commercial
24 Surveillance and Data Security” and published on August
25 22, 2022 (87 Fed. Reg. 51273) shall be terminated.

1 **SEC. 122. SEVERABILITY.**

2 If any provision of this title, or the application thereof
3 to any person or circumstance, is held invalid, the remain-
4 der of this title, and the application of such provision to
5 other persons not similarly situated or to other cir-
6 cumstances, may not be affected by the invalidation.

7 **SEC. 123. INNOVATION RULEMAKINGS.**

8 The Commission may conduct a rulemaking pursuant
9 to section 553 of title 5, United States Code—

10 (1) to include other covered data in the defini-
11 tion of the term “sensitive covered data”, except
12 that the Commission may not expand the category
13 of information described in section 101(49)(A)(ii);
14 and

15 (2) to include in the list of permitted purposes
16 in section 102(d) other permitted purposes for col-
17 lecting, processing, retaining, or transferring covered
18 data.

19 **SEC. 124. EFFECTIVE DATE.**

20 Unless otherwise specified in this title, this title shall
21 take effect on the date that is 180 days after the date
22 of the enactment of this Act.

1 **TITLE II—CHILDREN’S ONLINE**
2 **PRIVACY PROTECTION ACT 2.0**

3 **SEC. 201. SHORT TITLE.**

4 This title may be cited as the “Children’s Online Pri-
5 vacy Protection Act 2.0”.

6 **SEC. 202. ONLINE COLLECTION, USE, DISCLOSURE, AND DE-**
7 **LETION OF PERSONAL INFORMATION OF**
8 **CHILDREN.**

9 (a) DEFINITIONS.—Section 1302 of the Children’s
10 Online Privacy Protection Act of 1998 (15 U.S.C. 6501)
11 is amended—

12 (1) by amending paragraph (2) to read as fol-
13 lows:

14 “(2) OPERATOR.—The term ‘operator’—

15 “(A) means any person—

16 “(i) who, for commercial purposes, in
17 interstate or foreign commerce operates or
18 provides a website on the internet, an on-
19 line service, an online application, or a mo-
20 bile application; and

21 “(ii) who—

22 “(I) collects or maintains, either
23 directly or through a service provider,
24 personal information from or about

1 the users of that website, service, or
2 application;

3 “(II) allows another person to
4 collect personal information directly
5 from users of that website, service, or
6 application (in which case, the oper-
7 ator is deemed to have collected the
8 information); or

9 “(III) allows users of that
10 website, service, or application to pub-
11 licly disclose personal information (in
12 which case, the operator is deemed to
13 have collected the information); and

14 “(B) does not include any nonprofit entity
15 that would otherwise be exempt from coverage
16 under section 5 of the Federal Trade Commis-
17 sion Act (15 U.S.C. 45).”;

18 (2) in paragraph (4)—

19 (A) by amending subparagraph (A) to read
20 as follows:

21 “(A) the release of personal information
22 collected from a child by an operator for any
23 purpose, except where the personal information
24 is provided to a person other than an operator
25 who—

1 “(i) provides support for the internal
2 operations of the website, online service,
3 online application, or mobile application
4 (as defined in paragraph (8)(C)) of the op-
5 erator, excluding any activity relating to
6 targeted advertising or first-party adver-
7 tising (as such terms are defined in section
8 101 of the American Privacy Rights Act of
9 2024) to children; and

10 “(ii) does not disclose or use that per-
11 sonal information for any other purpose;
12 and”; and

13 (B) in subparagraph (B)—

14 (i) by striking “website or online serv-
15 ice” and inserting “website, online service,
16 online application, or mobile application”;
17 and

18 (ii) by striking “actual knowledge”
19 and inserting “actual knowledge or knowl-
20 edge fairly implied on the basis of objective
21 circumstances”;

22 (3) by striking paragraph (8) and inserting the
23 following:

24 “(8) PERSONAL INFORMATION.—

1 “(A) IN GENERAL.—The term ‘personal in-
2 formation’ means individually identifiable infor-
3 mation about an individual collected online, in-
4 cluding—

5 “(i) a first and last name;

6 “(ii) a home or other physical address
7 including street name and name of a city
8 or town;

9 “(iii) an e-mail address;

10 “(iv) a telephone number;

11 “(v) a Social Security number;

12 “(vi) any other identifier that the
13 Commission determines permits the phys-
14 ical or online contacting of a specific indi-
15 vidual;

16 “(vii) a persistent identifier that can
17 be used to recognize a specific child over
18 time and across different websites, online
19 services, online applications, or mobile ap-
20 plications, including a customer number
21 held in a cookie, an Internet Protocol (IP)
22 address, a processor or device serial num-
23 ber, or unique device identifier, but exclud-
24 ing an identifier that is used by an oper-
25 ator solely for providing support for the in-

1 ternal operations of the website, online
2 service, online application, or mobile appli-
3 cation;

4 “(viii) a photograph, video, or audio
5 file where such file contains a specific
6 child’s image or voice;

7 “(ix) geolocation information;

8 “(x) information generated from the
9 measurement or technological processing of
10 an individual’s biological, physical, or phys-
11 iological characteristics that is used to
12 identify an individual, including—

13 “(I) fingerprints;

14 “(II) voice prints;

15 “(III) iris or retina imagery
16 scans;

17 “(IV) facial templates;

18 “(V) deoxyribonucleic acid
19 (DNA) information; or

20 “(VI) gait; or

21 “(xi) information linked or reasonably
22 linkable to a child or the parents of that
23 child (including any unique identifier) that
24 an operator collects online from the child

1 and combines with an identifier described
2 in this subparagraph.

3 “(B) EXCLUSION.—The term ‘personal in-
4 formation’ does not include an audio file that
5 contains a child’s voice so long as the oper-
6 ator—

7 “(i) does not request information via
8 voice that would otherwise be considered
9 personal information under this paragraph;

10 “(ii) provides clear notice of its collec-
11 tion and use of the audio file and its dele-
12 tion policy in its privacy policy;

13 “(iii) only uses the voice within the
14 audio file solely as a replacement for writ-
15 ten words, to perform a task, or engage
16 with a website, online service, online appli-
17 cation, or mobile application, such as to
18 perform a search or fulfill a verbal instruc-
19 tion or request; and

20 “(iv) only maintains the audio file
21 long enough to complete the stated purpose
22 and then immediately deletes the audio file
23 and does not make any other use of the
24 audio file prior to deletion.

1 “(C) SUPPORT FOR THE INTERNAL OPER-
2 ATIONS OF A WEBSITE, ONLINE SERVICE, ON-
3 LINE APPLICATION, OR MOBILE APPLICATION.—

4 “(i) IN GENERAL.—For purposes of
5 subparagraph (A)(vii), the term ‘support
6 for the internal operations of a website, on-
7 line service, online application, or mobile
8 application’ means those activities nec-
9 essary to—

10 “(I) maintain or analyze the
11 functioning of the website, online serv-
12 ice, online application, or mobile appli-
13 cation;

14 “(II) perform network commu-
15 nications;

16 “(III) authenticate users of, or
17 personalize the content on, the
18 website, online service, online applica-
19 tion, or mobile application;

20 “(IV) cap the frequency of adver-
21 tising;

22 “(V) protect the security or in-
23 tegrity of the user, website, online
24 service, online application, or mobile
25 application;

1 “(VI) ensure legal or regulatory
2 compliance, or

3 “(VII) fulfill a request of a child
4 as permitted by subparagraphs (A)
5 through (C) of section 1303(b)(2).

6 “(ii) CONDITION.—Except as specifi-
7 cally permitted under clause (i), informa-
8 tion collected for the activities listed in
9 clause (i) may not be used or disclosed to
10 contact a specific individual, including
11 through targeted advertising or first-party
12 advertising (as such terms are defined in
13 section 101 of the American Privacy
14 Rights Act of 2024) to children, to amass
15 a profile on a specific individual, in connec-
16 tion with processes that encourage or
17 prompt use of a website or online service,
18 or for any other purpose.”;

19 (4) by amending paragraph (9) to read as fol-
20 lows:

21 “(9) VERIFIABLE CONSENT.—The term
22 ‘verifiable consent’ means any reasonable effort (tak-
23 ing into consideration available technology), includ-
24 ing a request for authorization for future collection,

1 use, and disclosure described in the notice, to ensure
2 that, a parent of the child—

3 “(A) receives direct notice of the personal
4 information collection, use, and disclosure prac-
5 tices of the operator; and

6 “(B) before the personal information of the
7 child is collected, freely and unambiguously au-
8 thorizes—

9 “(i) the collection, use, and disclosure,
10 as applicable, of that personal information;
11 and

12 “(ii) any subsequent use of that per-
13 sonal information.”;

14 (5) in paragraph (10)—

15 (A) in the paragraph heading, by striking
16 “WEBSITE OR ONLINE SERVICE DIRECTED TO
17 CHILDREN” and inserting “WEBSITE, ONLINE
18 SERVICE, ONLINE APPLICATION, OR MOBILE AP-
19 PPLICATION DIRECTED TO CHILDREN”;

20 (B) by striking “website or online service”
21 each place it appears and inserting “website,
22 online service, online application, or mobile ap-
23 plication”; and

24 (C) by adding at the end the following new
25 subparagraph:

1 “(C) RULE OF CONSTRUCTION.—In con-
2 sidering whether a website, online service, on-
3 line application, or mobile application, or por-
4 tion thereof, is directed to children, the Com-
5 mission shall apply a totality of circumstances
6 test and shall also consider competent and reli-
7 able empirical evidence regarding audience com-
8 position and evidence regarding the intended
9 audience of the website, online service, online
10 application, or mobile application.”; and

11 (6) by adding at the end the following:

12 “(13) CONNECTED DEVICE.—The term ‘con-
13 nected device’ has the meaning given such term in
14 section 101 of the American Privacy Rights Act of
15 2024.

16 “(14) ONLINE APPLICATION.—The term ‘online
17 application’ has the meaning given such term in sec-
18 tion 101 of the American Privacy Rights Act of
19 2024.

20 “(15) MOBILE APPLICATION.—The term ‘mo-
21 bile application’ has the meaning given such term in
22 section 101 of the American Privacy Rights Act of
23 2024.

24 “(16) PRECISE GEOLOCATION INFORMATION.—
25 The term ‘precise geolocation information’ has the

1 meaning given such term in section 101 of the
2 American Privacy Rights Act of 2024.

3 “(17) EDUCATIONAL AGENCY OR INSTITU-
4 TION.—The term ‘educational agency or institution’
5 means a State educational agency or local edu-
6 cational agency as defined under Federal law, as
7 well as an institutional day or residential school, in-
8 cluding a public school, charter school, or private
9 school, that provides elementary or secondary edu-
10 cation, as determined under State law.”.

11 (b) ONLINE COLLECTION, USE, DISCLOSURE, AND
12 DELETION OF PERSONAL INFORMATION OF CHILDREN.—
13 Section 1303 of the Children’s Online Privacy Protection
14 Act of 1998 (15 U.S.C. 6502) is amended—

15 (1) by striking the heading and inserting the
16 following: “**ONLINE COLLECTION, USE, AND DIS-**
17 **CLOSURE OF PERSONAL INFORMATION OF**
18 **CHILDREN.**”;

19 (2) in subsection (a)—

20 (A) by amending paragraph (1) to read as
21 follows:

22 “(1) IN GENERAL.—It is unlawful for an oper-
23 ator of a website, online service, online application,
24 or mobile application directed to children or for any
25 operator of a website, online service, online applica-

1 tion, or mobile application with actual knowledge or
2 knowledge fairly implied on the basis of objective cir-
3 cumstances that a user is a child—

4 “(A) to collect personal information from a
5 child in a manner that violates the American
6 Privacy Rights Act of 2024 or the regulations
7 prescribed under subsection (b); and

8 “(B) to store or transfer the personal in-
9 formation of a child outside of the United
10 States unless—

11 “(i) the operator provides direct notice
12 to the parent of the child that the child’s
13 personal information is being stored or
14 transferred outside of the United States;
15 and

16 “(ii) with respect to transfer, the op-
17 erator meets the requirements of section
18 102(b) of the American Privacy Rights Act
19 of 2024.”; and

20 (B) in paragraph (2), by striking “of such
21 a website or online service”;

22 (3) in subsection (b)—

23 (A) in paragraph (1)—

24 (i) in subparagraph (A)—

1 (I) in the matter preceding clause
2 (i), by striking “operator of any
3 website” and all that follows through
4 “from a child” and inserting “oper-
5 ator of a website, online service, on-
6 line application, or mobile application
7 directed to children or that has actual
8 knowledge or knowledge fairly implied
9 on the basis of objective circumstances
10 that a user is a child”;

11 (II) in clause (i)—

12 (aa) by striking “notice on
13 the website” and inserting “clear
14 and conspicuous notice on the
15 website”; and

16 (bb) by striking “; and” and
17 inserting a semicolon;

18 (III) in clause (ii), by striking
19 the semicolon at the end and inserting
20 “; and”; and

21 (IV) by inserting after clause (ii)
22 the following new clause:

23 “(iii) to obtain verifiable consent from
24 a parent of a child before using or dis-
25 closing personal information of the child

- 1 for any purpose that is a material change
2 from the original purposes and disclosure
3 practices specified to the parent of the
4 child under clause (i);”;
- 5 (ii) by striking subparagraph (B);
6 (iii) in subparagraph (C)—
- 7 (I) by striking “reasonably”; and
8 (II) by inserting “, proportionate,
9 and limited” after “necessary”; and
- 10 (iv) by redesignating subparagraphs
11 (C) and (D) as subparagraphs (B) and
12 (C), respectively;
13 (B) in paragraph (2)—
- 14 (i) in the matter preceding subpara-
15 graph (A), by striking “verifiable parental
16 consent” and inserting “verifiable con-
17 sent”;
- 18 (ii) in subparagraph (A), by inserting
19 “or to contact another child” after “to re-
20 contact the child”;
- 21 (iii) in subparagraph (B)—
- 22 (I) by striking “or child”; and
23 (II) by striking “parental con-
24 sent” each place the term appears and
25 inserting “verifiable consent”; and

1 (iv) in subparagraph (D), in the mat-
2 ter preceding clause (i)—

3 (I) by striking “reasonably”; and

4 (II) by inserting “, proportionate,
5 and limited” after “necessary”;

6 (C) by redesignating paragraph (3) as
7 paragraph (4) and inserting after paragraph
8 (2) the following new paragraph:

9 “(3) APPLICATION TO OPERATORS ACTING
10 UNDER AGREEMENTS WITH EDUCATIONAL AGENCIES
11 OR INSTITUTIONS.—The regulations may provide
12 that verifiable consent under paragraph (1)(A)(ii) is
13 not required for an operator that is acting under a
14 written agreement with an educational agency or in-
15 stitution that, at a minimum, requires the—

16 “(A) operator to—

17 “(i) limit its collection, use, and dis-
18 closure of the personal information from a
19 child to solely educational purposes and for
20 no other commercial purposes;

21 “(ii) provide the educational agency or
22 institution with a notice of the specific
23 types of personal information the operator
24 will collect from the child, the method by
25 which the operator will obtain the personal

1 information, and the purposes for which
2 the operator will collect, use, disclose, and
3 retain the personal information;

4 “(iii) provide the educational agency
5 or institution with a link to the operator’s
6 online notice of information practices as
7 required under paragraph (1)(A)(i); and

8 “(iv) provide the educational agency
9 or institution, upon request, with a means
10 to review the personal information collected
11 from a child, to prevent further use or
12 maintenance or future collection of per-
13 sonal information from a child, and to de-
14 delete personal information collected from a
15 child or content or information submitted
16 by a child to the operator’s website, online
17 service, online application, or mobile appli-
18 cation;

19 “(B) representative of the educational
20 agency or institution to acknowledge and agree
21 that they have authority to authorize the collec-
22 tion, use, and disclosure of personal information
23 from children on behalf of the educational agen-
24 cy or institution, along with such authorization,

1 their name, and title at the educational agency
2 or institution; and

3 “(C) educational agency or institution to—

4 “(i) provide on its website a notice
5 that identifies the operator with which it
6 has entered into a written agreement
7 under this paragraph and provides a link
8 to the operator’s online notice of informa-
9 tion practices as required under paragraph
10 (1)(A)(i);

11 “(ii) provide the operator’s notice re-
12 garding its information practices, as re-
13 quired under subparagraph (A)(ii), upon
14 request, to a parent; and

15 “(iii) upon the request of a parent, re-
16 quest the operator provide a means to re-
17 view the personal information from the
18 child and provide the parent a means to
19 review the personal information.”;

20 (D) by amending paragraph (4), as so re-
21 designated, to read as follows:

22 “(4) **TERMINATION OF SERVICE.**—The regula-
23 tions shall permit the operator of a website, online
24 service, online application, or mobile application di-
25 rected to children to terminate service provided to a

1 child whose parent has requested to delete covered
2 data of the child pursuant to section 105 of the
3 American Privacy Rights Act of 2024.”; and

4 (E) by adding at the end the following new
5 paragraphs:

6 “(5) CONTINUATION OF SERVICE.—The regula-
7 tions shall prohibit an operator from discontinuing
8 service provided to a child on the basis of a request
9 by the parent of the child to delete personal informa-
10 tion collected from the child, to the extent that the
11 operator is capable of providing such service without
12 such information.

13 “(6) COMMON VERIFIABLE CONSENT MECHA-
14 NISM.—

15 “(A) IN GENERAL.—

16 “(i) FEASIBILITY OF MECHANISM.—
17 The Commission shall assess the feasi-
18 bility, with notice and public comment, of
19 allowing operators the option to use a com-
20 mon verifiable consent mechanism that
21 fully meets the requirements of this title.

22 “(ii) REQUIREMENTS.—The feasibility
23 assessment described in clause (i) shall
24 consider whether a single operator could
25 use a common verifiable consent mecha-

1 nism to obtain verifiable consent, as re-
2 quired under this title, from a parent of a
3 child on behalf of multiple, listed operators
4 that provide a joint or related service.

5 “(B) REPORT.—Not later than 1 year
6 after the date of the enactment of this para-
7 graph, the Commission shall submit a report to
8 the Committee on Commerce, Science, and
9 Transportation of the Senate and the Com-
10 mittee on Energy and Commerce of the House
11 of Representatives with the findings of the as-
12 sessment required by subparagraph (A).

13 “(C) REGULATIONS.—If the Commission
14 finds that the use of a common verifiable con-
15 sent mechanism is feasible and would meet the
16 requirements of this title, the Commission shall
17 issue regulations to permit the use of a common
18 verifiable consent mechanism in accordance
19 with the findings outlined in such report.”;

20 (4) in subsection (c), by striking “a regulation
21 prescribed under subsection (a)” and inserting “sub-
22 paragraph (B) of subsection (a)(1), or of a regula-
23 tion prescribed under subsection (b),”; and

24 (5) by striking subsection (d) and inserting the
25 following:

1 “(d) RELATIONSHIP TO STATE LAW.—The provisions
2 of this title shall preempt any State law, rule, or regula-
3 tion only to the extent that such State law, rule, or regula-
4 tion conflicts with a provision of this title. Nothing in this
5 title shall be construed to prohibit any State from enacting
6 a law, rule, or regulation that provides greater protection
7 to children than the provisions of this title.”.

8 (c) SAFE HARBORS.—Section 1304 of the Children’s
9 Online Privacy Protection Act of 1998 (15 U.S.C. 6503)
10 is amended by adding at the end the following:

11 “(d) PUBLICATION.—

12 “(1) IN GENERAL.—Subject to the restrictions
13 described in paragraph (2), the Commission shall
14 publish on the internet website of the Commission
15 any report or documentation required by regulation
16 to be submitted to the Commission to carry out this
17 section.

18 “(2) RESTRICTIONS ON PUBLICATION.—The re-
19 strictions described in section 6(f) and section 21 of
20 the Federal Trade Commission Act (15 U.S.C.
21 46(f), 57b–2) applicable to the disclosure of infor-
22 mation obtained by the Commission shall apply in
23 same manner to the disclosure under this subsection
24 of information obtained by the Commission from a

1 report or documentation described in paragraph
2 (1).”.

3 (d) ACTIONS BY STATES.—Section 1305 of the Chil-
4 dren’s Online Privacy Protection Act of 1998 (15 U.S.C.
5 6504) is amended—

6 (1) in subsection (a)(1)—

7 (A) in the matter preceding subparagraph
8 (A), by inserting “section 1303(a)(1) or” before
9 “any regulation”; and

10 (B) in subparagraph (B), by inserting
11 “section 1303(a)(1) or” before “the regula-
12 tion”; and

13 (2) in subsection (d)—

14 (A) by inserting “section 1303(a)(1) or”
15 before “any regulation”; and

16 (B) by inserting “section 1303(a)(1) or”
17 before “that regulation”.

18 (e) ADMINISTRATION AND APPLICABILITY OF ACT.—
19 Section 1306 of the Children’s Online Privacy Protection
20 Act of 1998 (15 U.S.C. 6505) is amended—

21 (1) in subsection (d)—

22 (A) by inserting “section 1303(a)(1) or”
23 before “a rule”; and

1 (B) by striking “such rule” and inserting
2 “section 1303(a)(1) or a rule of the Commis-
3 sion under section 1303”; and

4 (2) by adding at the end the following new sub-
5 sections:

6 “(f) DETERMINATION OF WHETHER AN OPERATOR
7 HAS KNOWLEDGE FAIRLY IMPLIED ON THE BASIS OF
8 OBJECTIVE CIRCUMSTANCES.—

9 “(1) RULE OF CONSTRUCTION.—For purposes
10 of enforcing this title or a regulation promulgated
11 under this title, in making a determination as to
12 whether an operator has knowledge fairly implied on
13 the basis of objective circumstances that a specific
14 user is a child, the Commission or State attorneys
15 general shall rely on competent and reliable evi-
16 dence, taking into account the totality of the cir-
17 cumstances, including whether a reasonable and pru-
18 dent person under the circumstances would have
19 known that the user is a child. Nothing in this title,
20 including a determination described in the preceding
21 sentence, shall be construed to require an operator
22 to—

23 “(A) affirmatively collect any personal in-
24 formation with respect to the age of a child that

1 an operator is not already collecting in the nor-
2 mal course of business; or

3 “(B) implement an age gating or age
4 verification functionality.

5 “(2) COMMISSION GUIDANCE.—

6 “(A) IN GENERAL.—Not later than 180
7 days after the date of the enactment of this
8 subsection, the Commission shall issue guidance
9 to provide information, including best practices
10 and examples for operators to understand the
11 Commission’s determination of whether an op-
12 erator has knowledge fairly implied on the basis
13 of objective circumstances that a user is a child.

14 “(B) LIMITATION.—No guidance issued by
15 the Commission with respect to this title shall
16 confer any rights on any person, State, or local-
17 ity, nor shall operate to bind the Commission or
18 any person to the approach recommended in
19 such guidance. In any enforcement action
20 brought pursuant to this title, the Commission
21 or State attorney general, as applicable, shall
22 allege a specific violation of a provision of this
23 title. The Commission or State attorney gen-
24 eral, as applicable, may not base an enforce-
25 ment action on, or execute a consent order

1 based on, practices that are alleged to be incon-
2 sistent with any such guidance, unless the prac-
3 tices allegedly violate this title.

4 “(g) **ADDITIONAL REQUIREMENT.**—Any regulations
5 issued under this title shall include a description and anal-
6 ysis of the impact of proposed and final rules on small
7 entities per the Regulatory Flexibility Act of 1980 (5
8 U.S.C. 601 et seq.).”.

9 **SEC. 203. STUDY AND REPORTS OF MOBILE AND ONLINE**
10 **APPLICATION OVERSIGHT AND ENFORCE-**
11 **MENT.**

12 (a) **OVERSIGHT REPORT.**—Not later than 3 years
13 after the date of the enactment of this Act, the Federal
14 Trade Commission shall submit to the Committee on Com-
15 merce, Science, and Transportation of the Senate and the
16 Committee on Energy and Commerce of the House of
17 Representatives a report on the processes of platforms
18 that offer mobile and online applications for ensuring that,
19 of those applications that are websites, online services, on-
20 line applications, or mobile applications directed to chil-
21 dren, the applications operate in accordance with—

22 (1) this title, the amendments made by this
23 title, and rules promulgated under this title; and

24 (2) rules promulgated by the Commission under
25 section 18 of the Federal Trade Commission Act (15

1 U.S.C. 57a) relating to unfair or deceptive acts or
2 practices in marketing.

3 (b) ENFORCEMENT REPORT.—Not later than 1 year
4 after the date of the enactment of this Act, and each year
5 thereafter, the Federal Trade Commission shall submit to
6 the Committee on Commerce, Science, and Transportation
7 of the Senate and the Committee on Energy and Com-
8 merce of the House of Representatives a report that ad-
9 dresses, at a minimum—

10 (1) the number of actions brought by the Com-
11 mission during the reporting year to enforce the
12 Children’s Online Privacy Protection Act of 1998
13 (15 U.S.C. 6501) (referred to in this subsection as
14 the “Act”) and the outcome of each such action;

15 (2) the total number of investigations or inquir-
16 ies into potential violations of the Act; during the re-
17 porting year;

18 (3) the total number of open investigations or
19 inquiries into potential violations of the Act as of the
20 time the report is submitted;

21 (4) the number and nature of complaints re-
22 ceived by the Commission relating to an allegation
23 of a violation of the Act during the reporting year;
24 and

1 (5) policy or legislative recommendations to
2 strengthen online protections for children.

3 (c) REPORT BY THE INSPECTOR GENERAL.—

4 (1) IN GENERAL.—Not later than 2 years after
5 the date of the enactment of this Act, the Inspector
6 General of the Federal Trade Commission shall sub-
7 mit to the Federal Trade Commission and to the
8 Committee on Commerce, Science, and Transpor-
9 tation of the Senate and the Committee on Energy
10 and Commerce of the House of Representatives a re-
11 port regarding the safe harbor provisions in section
12 1304 of the Children’s Online Privacy Protection
13 Act of 1998 (15 U.S.C. 6503), which shall include—

14 (A) an analysis of whether the safe harbor
15 provisions are—

16 (i) operating fairly and effectively;

17 and

18 (ii) effectively protecting the interests
19 of children and minors; and

20 (B) any proposal or recommendation for
21 policy changes that would improve the effective-
22 ness of the safe harbor provisions.

23 (2) PUBLICATION.—Not later than 10 days
24 after the date on which a report is submitted under

1 paragraph (1), the Commission shall publish the re-
2 port on the website of the Commission.

3 **SEC. 204. SEVERABILITY.**

4 If any provision of this title, or an amendment made
5 by this title, is determined to be unenforceable or invalid,
6 the remaining provisions of this title and the amendments
7 made by this title may not be affected.