

118TH CONGRESS
2D SESSION

H. R. 8818

To provide Americans with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 25, 2024

Mrs. RODGERS of Washington (for herself, Mr. PALLONE, Mr. BILIRAKIS, and Ms. SCHAKOWSKY) introduced the following bill; which was referred to the Committee on Energy and Commerce

A BILL

To provide Americans with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement, 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.
- Sec. 105. Individual control over covered data.
- Sec. 106. Opt-out rights and universal mechanisms.
- Sec. 107. Interference with consumer rights.
- Sec. 108. Prohibition on denial of service and waiver of rights.
- Sec. 109. Data security and protection of covered data.
- Sec. 110. Executive responsibility.
- Sec. 111. Service providers and third parties.
- Sec. 112. Data brokers.
- Sec. 113. Commission-approved compliance guidelines.
- Sec. 114. Privacy-enhancing technology pilot program.
- Sec. 115. Enforcement by Federal Trade Commission.
- Sec. 116. Enforcement by States.
- Sec. 117. Enforcement by persons.
- Sec. 118. Relation to other laws.
- Sec. 119. Children’s Online Privacy Protection Act of 1998.
- Sec. 120. Data protections for covered minors.
- Sec. 121. Termination of FTC rulemaking on commercial surveillance and data security.
- Sec. 122. Severability.
- Sec. 123. Innovation rulemakings.
- Sec. 124. Effective date.

TITLE II—CHILDREN’S ONLINE PRIVACY PROTECTION ACT 2.0

- Sec. 201. Short title.
- Sec. 202. Online collection, use, disclosure, and deletion of personal information of children.
- Sec. 203. Study and reports on mobile and online application oversight and enforcement.
- Sec. 204. Severability.

1 **TITLE I—AMERICAN PRIVACY** 2 **RIGHTS**

3 **SEC. 101. DEFINITIONS.**

4 In this title:

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

6 (A) **IN GENERAL.**—The term “affirmative
7 express consent” means an affirmative act by
8 an individual that—

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

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

9 (B) REQUEST REQUIREMENTS.—The re-
10 quirements of this subparagraph with respect to
11 a request are the following:

12 (i) The request is provided to the indi-
13 vidual in a clear and conspicuous stand-
14 alone disclosure.

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

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

23 (II) clearly states the specific
24 categories of covered data that the
25 covered entity shall collect, process,

1 retain, or transfer under each such
2 act or practice; and

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

8 (iii) The request clearly explains the
9 applicable rights of the individual related
10 to consent.

11 (iv) The request is made in a manner
12 reasonably accessible to and usable by indi-
13 viduals living with disabilities.

14 (v) The request is made available to
15 the individual in the language in which the
16 covered entity provides a product or service
17 for which authorization is sought.

18 (vi) The option to refuse consent is at
19 least as prominent as the option to provide
20 consent, and the option to refuse consent
21 takes no more than 1 additional step as
22 compared to the number of steps necessary
23 to provide consent.

24 (vii) With respect to affirmative ex-
25 press consent sought for the collection,

1 processing, retention, or transfer of bio-
2 metric information or genetic information,
3 the request includes the length of time the
4 covered entity or service provider intends
5 to retain the biometric information or ge-
6 netic information or, if it is not possible to
7 identify the length of time, the criteria
8 used to determine the length of time the
9 covered entity or service provider intends
10 to retain the biometric information or ge-
11 netic information.

12 (C) EXPRESS CONSENT REQUIRED.—Af-
13 firmative express consent to an act or practice
14 may not be inferred from the inaction of an in-
15 dividual or the continued use by an individual
16 of a service or product provided by an entity.

17 (D) WITHDRAWAL OF AFFIRMATIVE EX-
18 PRESS CONSENT.—

19 (i) IN GENERAL.—A covered entity
20 shall provide an individual with a means to
21 withdraw affirmative express consent pre-
22 viously provided by the individual.

23 (ii) REQUIREMENTS.—The means to
24 withdraw affirmative express consent de-
25 scribed in clause (i) shall be—

1 (I) clear and conspicuous; and

2 (II) as easy for a reasonable indi-
3 vidual to use as the mechanism by
4 which the individual provided affirma-
5 tive express consent.

6 (E) CHILDREN AND TEENS.—If a covered
7 entity has knowledge that—

8 (i) an individual is a child, only a par-
9 ent of the child may provide affirmative ex-
10 press consent on behalf of the child; or

11 (ii) an individual is a teen, a parent or
12 the teen may provide affirmative express
13 consent on behalf of the teen.

14 (2) BIOMETRIC INFORMATION.—

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

22 (i) fingerprints;

23 (ii) voice prints;

24 (iii) iris or retina imagery scans;

1 (iv) facial or hand mapping, geometry,
2 or templates; and

3 (v) gait.

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

6 (i) a digital or physical photograph;

7 (ii) an audio or video recording; or

8 (iii) data derived from a digital or
9 physical photograph or an audio or video
10 recording that cannot be used to identify
11 or authenticate a specific individual.

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

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

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

1 than a geographic area equal to the area of a circle
2 with a radius of 1,850 feet).

3 (6) COLLECT.—The term “collect” means, with
4 respect to covered data, to buy, rent, gather, obtain,
5 receive, access, or otherwise acquire the covered data
6 by any means.

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

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

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

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

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

20 (B) is based solely on—

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

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

25 (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 such term in section 3 of the
5 Americans with Disabilities Act of 1990 (42 U.S.C.
6 12102).

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

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

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

21 (A) about an individual related to the
22 course of employment or application for employ-
23 ment of the individual (including on a contract
24 or temporary basis), if such information is col-
25 lected, retained, processed, or transferred by

1 the employer or the service provider of the em-
2 ployer solely for purposes necessary for the em-
3 ployment or application of the individual;

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

11 (C) about an individual who is an employee
12 or former employee of an employer, or a rel-
13 ative, dependent, or beneficiary of the employee
14 or former employee, and collected, retained,
15 processed, or transferred for the purpose of ad-
16 ministering benefits, including enrollment and
17 disenrollment for benefits, to which the em-
18 ployee, former employee, relative, dependent, or
19 beneficiary is entitled on the basis of the em-
20 ployment of the employee or former employee
21 with the employer, if such information is col-
22 lected, retained, processed, or transferred by
23 the employer or the service provider of the em-
24 ployer solely for the purpose of administering
25 such benefits.

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

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

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

14 (29) FIRST PARTY.—The term “first party”—

15 (A) means a consumer-facing covered enti-
16 ty with which a consumer intends and expects
17 to interact; and

18 (B) includes any entities with which the
19 covered entity shares common branding.

20 (30) FIRST-PARTY ADVERTISING.—

21 (A) IN GENERAL.—The term “first-party
22 advertising” means advertising or marketing by
23 a first party using the first-party data of the
24 first party and not other forms of covered data
25 and carried out—

1 (i) through direct communications
2 with an individual, such as direct mail,
3 email (subject to the CAN-SPAM Act of
4 2003 (15 U.S.C. 7701 et seq.) and the
5 regulations promulgated under such Act),
6 or text message communications (subject
7 to section 227 of the Communications Act
8 of 1934 (47 U.S.C. 227) and the regula-
9 tions promulgated under such section); or

10 (ii) entirely—

11 (I) in a physical location oper-
12 ated by the first party;

13 (II) in the case of a first party
14 that is not a covered high-impact so-
15 cial media company, on a website, on-
16 line service, online application, or mo-
17 bile application operated by the first
18 party, through display or presentation
19 of an online advertisement that pro-
20 motes a product or service (whether
21 offered by the first party or not of-
22 fered by the first party) to an indi-
23 vidual or device identified by a unique
24 persistent identifier, or group of indi-

1 viduals or devices identified by unique
2 persistent identifiers; or

3 (III) in the case of a first party
4 that is a covered high-impact social
5 media company, on a website, online
6 service, online application, or mobile
7 application operated by the first
8 party, through display or presentation
9 of an online advertisement that pro-
10 motes a product or service offered by
11 the first party to an individual or de-
12 vice identified by a unique persistent
13 identifier, or group of individuals or
14 devices identified by unique persistent
15 identifiers.

16 (B) EXCLUSION.—The term “first-party
17 advertising” does not include contextual adver-
18 tising.

19 (31) FIRST-PARTY DATA.—The term “first-
20 party data” means covered data collected directly
21 from an individual by a first party, including based
22 on a visit by the individual to or use by the indi-
23 vidual of a physical location, website, online service,
24 online application, or mobile application operated by
25 the first party.

1 (32) GENETIC INFORMATION.—The term “ge-
2 netic information” means any covered data, regard-
3 less of format, that concerns the genetic characteris-
4 tics of an identified or identifiable individual, includ-
5 ing—

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

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

13 (33) HEALTH INFORMATION.—The term
14 “health information” means information that de-
15 scribes or reveals the past, present, or future phys-
16 ical health, mental health, disability, diagnosis, or
17 health condition, status, or treatment of an indi-
18 vidual, including the precise geolocation information
19 of such treatment.

20 (34) INDIVIDUAL.—The term “individual”
21 means a natural person residing in the United
22 States.

23 (35) KNOWLEDGE.—

24 (A) IN GENERAL.—The term “knowledge”
25 means, with respect to whether an individual is

1 a child, teen, or covered minor, actual knowl-
2 edge or knowledge fairly implied on the basis of
3 objective circumstances.

4 (B) RULE OF CONSTRUCTION.—For pur-
5 poses of enforcing this title or a regulation pro-
6 mulgated under this title, a determination as to
7 whether a covered entity has knowledge fairly
8 implied on the basis of objective circumstances
9 that an individual is a child, teen, or covered
10 minor shall rely on competent and reliable evi-
11 dence, taking into account the totality of the
12 circumstances, including whether a reasonable
13 and prudent person under the circumstances
14 would have known that the individual is a child,
15 teen, or covered minor. Nothing in this title, in-
16 cluding a determination described in the pre-
17 ceding sentence, may be construed to require a
18 covered entity to—

19 (i) affirmatively collect any covered
20 data with respect to the age of a child,
21 teen, or covered minor that the covered en-
22 tity is not already collecting in the normal
23 course of business; or

24 (ii) implement an age gating or age
25 verification functionality.

1 (C) COMMISSION GUIDANCE.—

2 (i) IN GENERAL.—Not later than 180
3 days after the date of the enactment of
4 this Act, the Commission shall issue guid-
5 ance to provide information, including best
6 practices and examples, for covered entities
7 to use in understanding whether a covered
8 entity has knowledge fairly implied on the
9 basis of objective circumstances that an in-
10 dividual is a child, teen, or covered minor.

11 (ii) LIMITATION.—No guidance issued
12 by the Commission under clause (i) confers
13 any rights on any person, State, or local-
14 ity, or operates to bind the Commission or
15 any person, State, or locality to the ap-
16 proach recommended in such guidance.
17 Any enforcement action brought pursuant
18 to this title by the Commission, or by the
19 attorney general of a State, the chief con-
20 sumer protection officer of a State, or an
21 officer or office of a State authorized to
22 enforce privacy or data security laws appli-
23 cable to covered entities or service pro-
24 viders, shall allege a specific violation of a
25 provision of this title, and the Commission

1 or the attorney general, chief consumer
2 protection officer, or other authorized offi-
3 cer or office of the State, as applicable,
4 may not base an enforcement action on, or
5 as applicable execute a consent order based
6 on, practices that are alleged to be incon-
7 sistent with any such guidance, unless the
8 practices allegedly violate this title.

9 (36) LARGE DATA HOLDER.—

10 (A) IN GENERAL.—The term “large data
11 holder” means a covered entity or service pro-
12 vider that, in the most recent calendar year,
13 had an annual gross revenue of not less than
14 \$250,000,000 and, subject to subparagraph
15 (B), collected, processed, retained, or trans-
16 ferred—

17 (i) the covered data of—

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

20 (II) more than 15,000,000 port-
21 able connected devices that identify or
22 are linked or reasonably linkable to 1
23 or more individuals; or

24 (III) more than 35,000,000 con-
25 nected devices that identify or are

1 linked or reasonable linkable to 1 or
2 more individuals; or

3 (ii) the sensitive covered data of—

4 (I) more than 200,000 individ-
5 uals;

6 (II) more than 300,000 portable
7 connected devices that identify or are
8 linked or reasonable linkable to 1 or
9 more individuals; or

10 (III) more than 700,000 con-
11 nected devices that identify or are
12 linked or reasonably linkable to 1 or
13 more individuals.

14 (B) EXCLUSIONS.—For the purposes of
15 subparagraph (A), a covered entity or service
16 provider may not be considered a large data
17 holder solely on the basis of collecting, proc-
18 essing, retaining, or transferring to a service
19 provider—

20 (i) personal mailing or email address-
21 es;

22 (ii) personal telephone numbers;

23 (iii) log-in information of an indi-
24 vidual or device to allow the individual or

1 device to log in to an account administered
2 by the covered entity; or

3 (iv) in the case of a covered entity
4 that is a seller of goods or services (other
5 than an entity that facilitates payment,
6 such as a bank, credit card processor, mo-
7 bile payment system, or payment plat-
8 form), credit, debit, or mobile payment in-
9 formation necessary and used to initiate,
10 render, bill for, finalize, complete, or other-
11 wise facilitate payments for such goods or
12 services.

13 (C) DEFINITION OF ANNUAL GROSS REV-
14 ENUE.—For the purposes of subparagraph (A),
15 the term “annual gross revenue”, with respect
16 to a covered entity or service provider—

17 (i) means the gross receipts the cov-
18 ered entity or service provider received, in
19 whatever form from all sources, without
20 subtracting any costs or expenses; and

21 (ii) includes contributions, gifts,
22 grants, dues or other assessments, income
23 from investments, and proceeds from the
24 sale of real or personal property.

1 (37) MARKET RESEARCH.—The term “market
2 research” means the collection, processing, retention,
3 or transfer of covered data, with affirmative express
4 consent, that is necessary, proportionate, and limited
5 to measure and analyze the market or market trends
6 of products, services, advertising, or ideas, if the
7 covered data is not—

8 (A) integrated into any product or service;

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

11 (C) used for targeted advertising or to oth-
12 erwise market to any individual or device of an
13 individual.

14 (38) MATERIAL CHANGE.—The term “material
15 change” means, with respect to treatment of covered
16 data, a change by an entity that would likely affect
17 the decision of an individual to engage with and pro-
18 vide covered data to the entity, including providing
19 affirmative express consent for, or opting out of, the
20 collection, processing, retention, or transfer of cov-
21 ered data pertaining to such individual.

22 (39) MOBILE APPLICATION.—The term “mobile
23 application”—

24 (A) means a software program that runs
25 on the operating system of—

- 1 (i) a cellular telephone;
2 (ii) a tablet computer; or
3 (iii) a similar portable computing de-
4 vice that transmits data over a wireless
5 connection; and

6 (B) includes a service or application of-
7 fered via a connected device.

8 (40) ON-DEVICE DATA.—

9 (A) IN GENERAL.—The term “on-device
10 data” means data collected, retained, and proc-
11 essed solely on the device of an individual.

12 (B) LIMITATION.—Data collected, re-
13 tained, and processed solely on the device of an
14 individual may be considered “on-device data”
15 only if—

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

18 (ii) the relevant covered entity clearly
19 and conspicuously provides the device
20 owner with controls that allow the owner
21 to access, correct, delete, and export such
22 data consistent with the rights provided
23 with respect to covered data pursuant to
24 section 105;

1 (iii) the relevant covered entity pro-
2 vides easy-to-understand instructions on
3 how the device owner can access such con-
4 trols; and

5 (iv) the relevant covered entity estab-
6 lishes, implements, and maintains reason-
7 able data security practices, consistent
8 with section 109, to protect—

9 (I) the confidentiality, integrity,
10 and availability of the on-device data;
11 and

12 (II) on device data against unau-
13 thorized access.

14 (41) ONLINE ACTIVITY PROFILE.—The term
15 “online activity profile” means covered data that
16 identifies the online activities of an individual (or a
17 device linked or reasonably linkable to an individual)
18 over time and across third-party websites, online
19 services, online applications, or mobile applications
20 that do not share common branding and that is col-
21 lected, processed, retained, or transferred for the
22 purpose of evaluating, analyzing, or predicting the
23 behaviors or characteristics of an individual.

24 (42) ONLINE APPLICATION.—The term “online
25 application”—

1 (A) means an internet-connected software
2 program; and

3 (B) includes a service or application of-
4 fered via a connected device.

5 (43) PARENT.—The term “parent” means a
6 legal guardian.

7 (44) PORTABLE CONNECTED DEVICE.—The
8 term “portable connected device” means a portable
9 device that is capable of connecting to the internet
10 over a wireless connection, including a smartphone,
11 tablet computer, laptop computer, smartwatch, or
12 similar portable device.

13 (45) PRECISE GEOLOCATION INFORMATION.—

14 (A) IN GENERAL.—The term “precise
15 geolocation information” means information
16 that reveals the past or present physical loca-
17 tion of an individual or device with sufficient
18 precision to identify the location of such indi-
19 vidual or device within a geographic area that
20 is equal to or less than the area of a circle with
21 a radius of 1,850 feet or less.

22 (B) EXCLUSIONS.—The term “precise
23 geolocation information” does not include infor-
24 mation derived solely from—

25 (i) a digital or physical photograph;

- 1 (ii) an audio or visual recording; or
2 (iii) metadata associated with a digital
3 or physical photograph or an audio or vis-
4 ual recording that cannot be linked to an
5 individual.

6 (46) PROCESS.—The term “process” means,
7 with respect to covered data, any operation or set of
8 operations performed on the covered data, including
9 analyzing, organizing, structuring, using, modifying,
10 or otherwise handling the covered data.

11 (47) PUBLICLY AVAILABLE INFORMATION.—

12 (A) IN GENERAL.—The term “publicly
13 available information” means any information
14 that a covered entity has a reasonable basis to
15 believe has been lawfully made available to the
16 general public by—

- 17 (i) Federal, State, or local government
18 records, if the covered entity collects, proc-
19 esses, retains, and transfers such informa-
20 tion in accordance with any restrictions or
21 terms of use placed on the information by
22 the relevant government entity;
- 23 (ii) widely distributed media;
- 24 (iii) a website or online service made
25 available to all members of the public, for

1 free or for a fee, including where all mem-
2 bers of the public can log in to the website
3 or online service; or

4 (iv) a disclosure to the general public
5 that is required to be made by Federal,
6 State, or local law.

7 (B) CLARIFICATIONS; LIMITATIONS.—

8 (i) AVAILABLE TO ALL MEMBERS OF
9 THE PUBLIC.—For purposes of this para-
10 graph, information from a website or on-
11 line service is not available to all members
12 of the public if the individual to whom the
13 information pertains has restricted the in-
14 formation to a specific audience or main-
15 tained a default setting that restricts the
16 information to a specific audience.

17 (ii) BUSINESS CONTACT INFORMA-
18 TION.—The term “publicly available infor-
19 mation” includes business contact informa-
20 tion of an individual acting in a business
21 or professional context that is made avail-
22 able on a website or online service made
23 available to all members of the public, in-
24 cluding the name, position or title, busi-
25 ness telephone number, business email ad-

1 dress, or business address of the indi-
2 vidual.

3 (iii) OTHER LIMITATIONS.—The term
4 “publicly available information” does not
5 include—

6 (I) any obscene visual depiction
7 (as such term is used in section 1460
8 of title 18, United States Code);

9 (II) derived data from publicly
10 available information that reveals in-
11 formation about an individual that
12 meets the definition of the term “sen-
13 sitive covered data”;

14 (III) biometric information;

15 (IV) genetic information, unless
16 made publicly available by the indi-
17 vidual to whom the information per-
18 tains by a means described in clause
19 (ii) or (iii) of subparagraph (A);

20 (V) covered data that is created
21 through the combination of covered
22 data with publicly available informa-
23 tion;

1 (VI) intimate images, authentic
2 or computer-generated, known to be
3 nonconsensual; or

4 (VII) sensitive covered data made
5 available by a data broker.

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

9 (49) SENSITIVE COVERED DATA.—

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

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

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

23 (iii) Genetic information.

24 (iv) A financial account number, debit
25 card number, credit card number, or any

1 required security or access code, password,
2 or credentials allowing access to any such
3 account or card, except that the last four
4 digits of an account number, debit card
5 number, or credit card number may not be
6 considered sensitive covered data.

7 (v) Biometric information.

8 (vi) Precise geolocation information.

9 (vii) The private communications of
10 an individual (such as voicemails, or other
11 voice or video communications, emails,
12 texts, direct messages, or mail) or informa-
13 tion identifying the parties to such commu-
14 nications, information contained in tele-
15 phone bills, and any information that per-
16 tains to the transmission of private voice
17 or video communications, including num-
18 bers called, numbers from which calls were
19 placed, the time calls were made, call dura-
20 tion, and location information of the par-
21 ties to the call, unless the relevant covered
22 entity or service provider is an intended re-
23 cipient of the communication.

24 (viii) Unencrypted or unredacted ac-
25 count or device log-in credentials.

1 (ix) Information revealing the sexual
2 behavior of an individual in a manner in-
3 consistent with the reasonable expectation
4 of the individual regarding disclosure of
5 such information.

6 (x) Calendar information, address
7 book information, phone, text, or electronic
8 logs, photographs, audio recordings, or vid-
9 eos intended for private use.

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

14 (xii) Information revealing the extent
15 or content of the access, viewing, or other
16 use by an individual of any video program-
17 ming (as defined in section 713(h)(2) of
18 the Communications Act of 1934 (47
19 U.S.C. 613(h)(2))), including program-
20 ming provided by a provider of broadcast
21 television service, cable service, satellite
22 service, or streaming media service, but
23 only with regard to the transfer of such in-
24 formation to a third party (excluding any

1 such information used solely for transfers
2 for independent video measurement).

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

10 (xiv) Information revealing the race,
11 ethnicity, national origin, religion, or sex of
12 an individual in a manner inconsistent
13 with the reasonable expectation of the indi-
14 vidual regarding disclosure of such infor-
15 mation.

16 (xv) An online activity profile.

17 (xvi) Information about a covered
18 minor.

19 (xvii) Information that reveals the sta-
20 tus of an individual as a member of the
21 Armed Forces.

22 (xviii) Neural data.

23 (xix) Any other covered data collected,
24 processed, retained, or transferred for the
25 purpose of identifying a type of informa-

1 tion described in any of clauses (i) through
2 (xviii).

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

6 (i) is related by common ownership or
7 corporate control to the provider of broad-
8 cast television service or streaming media
9 service; and

10 (ii) provides video programming as de-
11 scribed in such subparagraph.

12 (50) SERVICE PROVIDER.—

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

18 (i) a covered entity or another service
19 provider; or

20 (ii) a Federal, State, Tribal, or local
21 government entity.

22 (B) RULE OF CONSTRUCTION.—

23 (i) IN GENERAL.—An entity is a cov-
24 ered entity and not a service provider with
25 respect to a specific collecting, processing,

1 retaining, or transferring of covered data,
2 if the entity, alone or jointly with others,
3 determines the purposes and means of the
4 specific collecting, processing, retaining, or
5 transferring of data.

6 (ii) INSTRUCTIONS.—An entity that is
7 not limited in its collecting, processing, re-
8 taining, or transferring of covered data
9 pursuant to the instructions of a covered
10 entity, another service provider, or a Fed-
11 eral, State, Tribal, or local government en-
12 tity, or that fails to adhere to such instruc-
13 tions, is a covered entity and not a service
14 provider with respect to a specific col-
15 lecting, processing, retaining, or transfer-
16 ring of such data. If a service provider be-
17 gins, alone or jointly with others, deter-
18 mining the purposes and means of col-
19 lecting, processing, retaining, or transfer-
20 ring covered data, the entity is a covered
21 entity with respect to such data.

22 (iii) CONTEXT REQUIRED.—Whether
23 an entity is a covered entity or a service
24 provider depends on the facts surrounding

1 how, and the context in which, data is col-
2 lected, processed, retained, or transferred.

3 (51) SMALL BUSINESS.—

4 (A) IN GENERAL.—The term “small busi-
5 ness” means an entity (including any affiliate
6 of the entity)—

7 (i) that has average annual gross rev-
8 enues for the period of the 3 preceding cal-
9 endar years (or for the period during
10 which the entity has been in existence, if
11 such period is less than 3 calendar years)
12 not exceeding \$40,000,000, indexed to the
13 Producer Price Index reported by the Bu-
14 reau of Labor Statistics;

15 (ii) that, on average for the period de-
16 scribed in clause (i), did not annually col-
17 lect, process, retain, or transfer the cov-
18 ered data of more than 200,000 individuals
19 for any purpose other than initiating, ren-
20 dering, billing for, finalizing, completing,
21 or otherwise collecting payment for a re-
22 quested service or product; and

23 (iii) that did not, during the period
24 described in clause (i), transfer covered
25 data to a third party in exchange for rev-

1 enue or anything of value, except for pur-
2 poses of initiating, rendering, billing for, fi-
3 nalizing, completing, or otherwise collecting
4 payment for a requested service or product
5 or facilitating web analytics that are not
6 used to create an online activity profile.

7 (B) NONPROFIT REVENUE.—For purposes
8 of subparagraph (A)(i), the term “revenue”, as
9 such term relates to any entity that is not orga-
10 nized to carry on business for its own profit or
11 that of its members, means the gross receipts
12 the entity received, in whatever form from all
13 sources, without subtracting any costs or ex-
14 penses, and includes contributions, gifts, grants
15 (except for grants from the Federal Govern-
16 ment), dues or other assessments, income from
17 investments, or proceeds from the sale of real
18 or personal property.

19 (52) STATE.—The term “State” means each of
20 the 50 States, the District of Columbia, the Com-
21 monwealth of Puerto Rico, the Virgin Islands of the
22 United States, Guam, American Samoa, and the
23 Commonwealth of the Northern Mariana Islands.

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

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

3 (B) any alleged physical or mental harm to
4 an individual that involves—

5 (i) treatment by a licensed,
6 credentialed, or otherwise bona fide health
7 care provider, hospital, community health
8 center, clinic, hospice, or residential or out-
9 patient facility for medical, mental health,
10 or addiction care; or

11 (ii) physical injury, highly offensive
12 intrusion into the privacy expectations of a
13 reasonable individual under the cir-
14 cumstances, or discrimination on the basis
15 of race, color, religion, national origin, sex,
16 or disability.

17 (54) TARGETED ADVERTISING.—The term “tar-
18 geted advertising”—

19 (A) means displaying or presenting an on-
20 line advertisement to an individual or to a de-
21 vice identified by a unique persistent identifier
22 (or to a group of individuals or devices identi-
23 fied by unique persistent identifiers), if the ad-
24 vertisement is selected based, in whole or in

1 part, on known or predicted preferences or in-
2 terests associated with the individual or device;

3 (B) includes—

4 (i) an online advertisement by a cov-
5 ered high-impact social media company for
6 a product or service that is not a product
7 or service offered by the covered high-im-
8 pact social media company; and

9 (ii) an online advertisement for a
10 product or service based on the previous
11 interaction of an individual or a device
12 identified by a unique persistent identifier
13 with such product or service on a website
14 or online service that does not share com-
15 mon branding or affiliation with the
16 website or online service displaying or pre-
17 senting the advertisement; and

18 (C) excludes contextual advertising and
19 first-party advertising.

20 (55) TEEN.—The term “teen” means an indi-
21 vidual 13 years of age or older, but under the age
22 of 17.

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

24 (A) means any entity that—

1 (i) receives covered data from another
2 entity that is not the individual to whom
3 the data pertains; and

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

6 (B) does not include an entity that collects
7 covered data from another entity if the 2 enti-
8 ties are—

9 (i) related by common ownership or
10 corporate control; or

11 (ii) nonprofit entities that are part of
12 the same federated nonprofit organization.

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

16 (58) TRANSFER.—The term “transfer” means,
17 with respect to covered data, to disclose, release,
18 share, disseminate, make available, sell, rent, or li-
19 cense the covered data (orally, in writing, electroni-
20 cally, or by any other means) for consideration of
21 any kind or for a commercial purpose.

22 (59) UNIQUE PERSISTENT IDENTIFIER.—

23 (A) IN GENERAL.—The term “unique per-
24 sistent identifier” means a technologically cre-
25 ated identifier to the extent that such identifier

1 is reasonably linkable to an individual or a de-
2 vice that identifies or is linked or reasonably
3 linkable to 1 or more individuals, including de-
4 vice identifiers, Internet Protocol addresses,
5 cookies, beacons, pixel tags, mobile ad identi-
6 fiers or similar technology customer numbers,
7 unique pseudonyms, user aliases, telephone
8 numbers, or other forms of persistent or prob-
9 abilistic identifiers that are linked or reasonably
10 linkable to 1 or more individuals or devices.

11 (B) EXCLUSION.—The term “unique per-
12 sistent identifier” does not include an identifier
13 assigned by a covered entity for the sole pur-
14 pose of giving effect to the exercise of affirma-
15 tive express consent or opt out by an individual
16 with respect to the collecting, processing, re-
17 taining, and transfer of covered data or other-
18 wise limiting the collecting, processing, retain-
19 ing, or transfer of covered data.

20 (60) WIDELY DISTRIBUTED MEDIA.—

21 (A) IN GENERAL.—The term “widely dis-
22 tributed media” means information that is
23 available to the general public, including infor-
24 mation from a telephone book or online direc-
25 tory, a television, internet, or radio program,

1 the news media, or an internet site that is avail-
2 able to the general public on an unrestricted
3 basis.

4 (B) EXCLUSION.—The term “widely dis-
5 tributed media” does not include an obscene
6 visual depiction (as such term is used in section
7 1460 of title 18, United States Code).

8 **SEC. 102. DATA MINIMIZATION.**

9 (a) IN GENERAL.—A covered entity may not collect,
10 process, retain, or transfer covered data of an individual
11 or direct a service provider to collect, process, retain, or
12 transfer covered data of an individual beyond what is nec-
13 essary, proportionate, and limited—

14 (1) to provide or maintain—

15 (A) a specific product or service requested
16 by the individual to whom the data pertains, in-
17 cluding any associated routine administrative,
18 operational, or account-servicing activity, such
19 as billing, shipping, delivery, storage, or ac-
20 counting; or

21 (B) a communication, that is not an adver-
22 tisement, by the covered entity to the individual
23 reasonably anticipated within the context of the
24 relationship; or

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

3 (b) ADDITIONAL PROTECTIONS FOR SENSITIVE COV-
4 ERED DATA.—Subject to subsection (a), a covered entity
5 may not transfer sensitive covered data to a third party
6 or direct a service provider to transfer sensitive covered
7 data to a third party without the affirmative express con-
8 sent of the individual to whom such data pertains, unless
9 for a purpose permitted by paragraph (2), (3), (4), (5),
10 (6), (8), (9), (11), (12), or (13) of subsection (d).

11 (c) ADDITIONAL PROTECTIONS FOR BIOMETRIC IN-
12 FORMATION AND GENETIC INFORMATION.—

13 (1) COLLECTION.—Subject to subsection (a), a
14 covered entity may not collect biometric information
15 or genetic information or direct a service provider to
16 collect biometric information or genetic information
17 without the affirmative express consent of the indi-
18 vidual to whom such information pertains.

19 (2) PROCESSING.—Subject to subsection (a), a
20 covered entity may not process biometric information
21 or genetic information or direct a service provider to
22 process biometric information or genetic information
23 without the affirmative express consent of the indi-
24 vidual to whom such information pertains, unless for

1 a purpose permitted by paragraph (2), (3), or (4) of
2 subsection (d).

3 (3) RETENTION.—Subject to subsection (a), a
4 covered entity may not retain biometric information
5 or direct a service provider to retain biometric infor-
6 mation beyond the point at which the purpose for
7 which an individual provided affirmative express
8 consent under paragraph (1) has been satisfied or
9 beyond the date that is 3 years after the date of the
10 last interaction of the individual with the covered en-
11 tity or service provider, whichever occurs first, un-
12 less for a purpose permitted under paragraph (2),
13 (3), or (4) of subsection (d).

14 (4) TRANSFER.—

15 (A) AFFIRMATIVE EXPRESS CONSENT RE-
16 QUIRED.—Subject to subsection (a), a covered
17 entity may not transfer biometric information
18 or genetic information to a third party or direct
19 a service provider to transfer biometric informa-
20 tion or genetic information to a third party
21 without the affirmative express consent of the
22 individual to whom such information pertains,
23 unless for a purpose permitted by paragraph
24 (2), (3), or (4) of subsection (d).

1 (B) NO TRANSFER FOR PAYMENT OR
2 OTHER VALUABLE CONSIDERATION.—A covered
3 entity may not transfer biometric information
4 or genetic information to a third party, or di-
5 rect a service provider to transfer biometric in-
6 formation or genetic information to a third
7 party, for payment or other valuable consider-
8 ation (regardless of the purpose of the transfer,
9 including a purpose described in subparagraph
10 (A)).

11 (d) PERMITTED PURPOSES.—Subject to the require-
12 ments in subsections (b) and (c), a covered entity may
13 collect, process, retain, or transfer or direct a service pro-
14 vider to collect, process, retain, or transfer covered data
15 for the following purposes, if the covered entity or service
16 provider can demonstrate that the collection, processing,
17 retention, or transfer is necessary, proportionate, and lim-
18 ited to such purpose:

19 (1) To protect data security as described in sec-
20 tion 109, protect against spam, or protect and main-
21 tain networks and systems, including through
22 diagnostics, debugging, and repairs.

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

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

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

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

10 (6) To conduct market research.

11 (7) With respect to covered data previously col-
12 lected in accordance with this title, to process the
13 covered data such that the covered data becomes de-
14 identified data, including in order to—

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

17 (B) conduct research or analytics to im-
18 prove a product or service of the covered entity
19 or service provider;

20 (C) conduct research to investigate, estab-
21 lish, or improve the effectiveness or safety of
22 medical products, including drugs, biologics,
23 and medical devices;

24 (D) enable the effective delivery and ad-
25 ministration of health care products and treat-

1 ments to patients, in compliance with Federal
2 regulations; or

3 (E) monitor the safety and efficacy of
4 health care products and services administered
5 to patients, in compliance with Federal regula-
6 tions.

7 (8) To transfer assets to a third party in the
8 context of a merger, acquisition, bankruptcy, or
9 similar transaction, with respect to which the third
10 party assumes control, in whole or in part, of the as-
11 sets of the covered entity, but only if the covered en-
12 tity, in a reasonable time prior to such transfer, pro-
13 vides each affected individual with—

14 (A) a notice describing such transfer, in-
15 cluding the name of the entity or entities receiv-
16 ing the covered data of the individual and the
17 privacy policies of such entity or entities as de-
18 scribed in section 104; and

19 (B) a reasonable opportunity to—

20 (i) withdraw any previously provided
21 consent in accordance with the require-
22 ments of affirmative express consent under
23 this title related to the covered data of the
24 individual; and

1 (ii) request the deletion of the covered
2 data of the individual, as described in sec-
3 tion 105.

4 (9) With respect to a covered entity or service
5 provider that is a telecommunications carrier or a
6 provider of a mobile service, interconnected VoIP
7 service, or non-interconnected VoIP service (as such
8 terms are defined in section 3 of the Communica-
9 tions Act of 1934 (47 U.S.C. 153)), to provide call
10 location information in a manner described in sub-
11 paragraph (A) or (C) of section 222(d)(4) of such
12 Act (47 U.S.C. 222(d)(4)).

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

17 (11) To prevent, detect, protect against, inves-
18 tigate, or respond to an ongoing or imminent secu-
19 rity incident relating to network security or physical
20 security, including an intrusion or trespass, medical
21 alert or request for a medical response, fire alarm or
22 request for a fire response, or access control.

23 (12) To prevent, detect, protect against, inves-
24 tigate, or respond to an imminent or ongoing public
25 safety incident (such as a mass casualty event, nat-

1 ural disaster, or national security incident), exclud-
2 ing the transfer of covered data for payment or
3 other valuable consideration to a government entity.

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

9 (14) Except with respect to sensitive covered
10 data, and only with respect to covered data pre-
11 viously collected in accordance with this title, to
12 process or transfer such data to provide first-party
13 advertising or contextual advertising or to measure
14 and report on marketing performance or media per-
15 formance by the covered entity, including processing
16 or transferring covered data for measurement and
17 reporting of frequency, attribution, and performance,
18 including by independent entities, except that this
19 paragraph does not permit the processing or trans-
20 fer of covered data for first-party advertising to a
21 covered minor as prohibited by section 120.

22 (15) Except with respect to sensitive covered
23 data, and only with respect to covered data pre-
24 viously collected in accordance with this title, to
25 process or transfer such data to provide targeted ad-

1 advertising, direct mail targeted advertising, or email
2 targeted advertising (subject to the CAN-SPAM Act
3 of 2003 (15 U.S.C. 7701 et seq.) and the regula-
4 tions promulgated under such Act) or to measure
5 and report on marketing performance or media per-
6 formance, including processing or transferring cov-
7 ered data for measurement and reporting of fre-
8 quency, attribution, and performance, including by
9 independent entities, except that this paragraph does
10 not permit the processing or transfer of covered data
11 for targeted advertising to an individual who has
12 opted out of targeted advertising pursuant to section
13 106 or to a covered minor as prohibited by section
14 120.

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

18 (A) is in the public interest;

19 (B) adheres to all relevant laws and regu-
20 lations governing such research, including regu-
21 lations for the protection of human subjects, if
22 applicable;

23 (C) limits transfers to third parties of sen-
24 sitive covered data to only those transfers nec-

1 essary, proportionate, and limited to carry out
2 the research; and

3 (D) prohibits the transfer of covered data
4 to a data broker.

5 (17) To conduct medical research in compliance
6 with part 46 of title 45, Code of Federal Regula-
7 tions, or parts 50 and 56 of title 21, Code of Fed-
8 eral Regulations.

9 (e) GUIDANCE.—Not later than 180 days after the
10 date of the enactment of this Act, the Commission shall
11 issue guidance regarding what is necessary, proportionate,
12 and limited to comply with this section.

13 (f) JOURNALISM.—Nothing in this title may be con-
14 strued to limit or diminish journalism, including gath-
15 ering, preparing, collecting, photographing, recording,
16 writing, editing, reporting, or investigating news or infor-
17 mation that concerns local, national, or international
18 events or other matters of public interest for dissemination
19 to the public.

20 **SEC. 103. PRIVACY BY DESIGN.**

21 (a) IN GENERAL.—Each covered entity and service
22 provider shall establish, implement, and maintain reason-
23 able policies, practices, and procedures that reflect the role
24 of the covered entity or service provider in the collection,
25 processing, retention, and transferring of covered data.

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

3 (1) identify, assess, and mitigate privacy risks
4 related to covered minors (including, if applicable, in
5 a manner that considers the developmental needs of
6 different age ranges of covered minors), individuals
7 living with disabilities, and individuals over the age
8 of 65;

9 (2) mitigate privacy risks related to the prod-
10 ucts and services of the covered entity or service pro-
11 vider, including in the design, development, and im-
12 plementation of such products and services, taking
13 into account the role of the covered entity or service
14 provider and the information available to the covered
15 entity or service provider; and

16 (3) implement reasonable internal training and
17 safeguards to promote compliance with this title and
18 to mitigate privacy risks, taking into account the
19 role of the covered entity or service provider and the
20 information available to the covered entity or service
21 provider.

22 (c) FACTORS TO CONSIDER.—The policies, practices,
23 and procedures established by a covered entity or service
24 provider under subsection (a) shall align with, as applica-
25 ble—

1 (1) the nature, scope, and complexity of the ac-
2 tivities engaged in by the covered entity or service
3 provider, including whether the covered entity or
4 service provider is a large data holder, nonprofit or-
5 ganization, or data broker, taking into account the
6 role of the covered entity or service provider and the
7 information available to the covered entity or service
8 provider;

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

12 (3) the volume of covered data collected, proc-
13 essed, retained, or transferred by the covered entity
14 or service provider;

15 (4) the number of individuals and devices to
16 which the covered data collected, processed, retained,
17 or transferred by the covered entity or service pro-
18 vider relates;

19 (5) state-of-the-art administrative, techno-
20 logical, and organizational measures that, by default,
21 serve the purpose of protecting the privacy and secu-
22 rity of covered data as required by this title; and

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

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

8 **SEC. 104. TRANSPARENCY.**

9 (a) IN GENERAL.—Each covered entity and service
10 provider shall make publicly available a clear and con-
11 spicuous, not misleading, and easy-to-read privacy policy
12 that provides a detailed and accurate representation of the
13 data collection, processing, retention, and transfer activi-
14 ties of the covered entity or service provider.

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

18 (1) The identity and the contact information
19 of—

20 (A) the covered entity or service provider
21 to which the privacy policy applies, including a
22 point of contact and a monitored email address
23 or other monitored online contact mechanism,
24 as applicable, specific to data privacy and data
25 security inquiries; and

1 (B) any affiliate within the same corporate
2 structure as the covered entity or service pro-
3 vider, to which the covered entity or service pro-
4 vider may transfer data, that—

5 (i) is not under common branding
6 with the covered entity or service provider;
7 or

8 (ii) has different contact information
9 than the covered entity or service provider.

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

12 (A) the categories of covered data the cov-
13 ered entity or service provider collects, proc-
14 esses, or retains; and

15 (B) the processing purposes for each such
16 category of covered data.

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

19 (A) each category of service provider or
20 third party to which the covered entity or serv-
21 ice provider transfers covered data;

22 (B) the name of each data broker to which
23 the covered entity or service provider transfers
24 covered data; and

1 (C) the purposes for which such data is
2 transferred.

3 (4) The length of time the covered entity or
4 service provider intends to retain each category of
5 covered data or, if it is not possible to identify the
6 length of time, the criteria used to determine the
7 length of time the covered entity or service provider
8 intends to retain each category of covered data.

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

12 (6) A description of how the covered entity
13 treats data collected from covered minors differently
14 than data collected from other individuals, if the
15 covered entity has knowledge that the covered entity
16 has collected data from covered minors.

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

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

20 (9) Whether any covered data collected by the
21 covered entity or service provider is transferred to,
22 processed in, retained in, or otherwise accessible to
23 a foreign adversary (as determined by the Secretary
24 of Commerce and specified in section 7.4 of title 15,

1 Code of Federal Regulations (or any successor regu-
2 lation)).

3 (c) LANGUAGES.—A privacy policy required under
4 subsection (a) shall be made available to the public—

5 (1) in the 10 most-used languages in which a
6 covered entity or service provider provides products
7 or services or carries out activities related to such
8 products or services; or

9 (2) if the covered entity or service provider pro-
10 vides products or services in fewer than 10 lan-
11 guages, in the languages in which the covered entity
12 or service provider provides products or services or
13 carries out activities related to such products or
14 services.

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

19 (e) MATERIAL CHANGES.—

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

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

1 (i) advance notice of such material
2 change; and

3 (ii) a means to opt out of the collec-
4 tion, processing, retention, or transfer of
5 any covered data of such individual pursu-
6 ant to such material change; and

7 (B) with respect to the covered data of any
8 individual who opts out using the means de-
9 scribed in subparagraph (A)(ii), discontinue the
10 collection, processing, retention, or transfer of
11 such covered data, unless such collection, proc-
12 essing, retention, or transfer is necessary, pro-
13 portionate, and limited to provide or maintain
14 a product or service specifically requested by
15 the individual.

16 (2) DIRECT NOTIFICATION.—A covered entity
17 shall take all reasonable electronic measures to pro-
18 vide direct notification, if possible, to each affected
19 individual regarding material changes to the privacy
20 policy of the covered entity, and such notification
21 shall be provided in each language in which the pri-
22 vacy policy is made available, taking into account
23 available technology and the nature of the relation-
24 ship between the covered entity and the individual.

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

5 (f) TRANSPARENCY REQUIREMENTS FOR LARGE
6 DATA HOLDERS.—

7 (1) RETENTION OF PRIVACY POLICIES; LOG OF
8 MATERIAL CHANGES.—

9 (A) IN GENERAL.—Beginning on the date
10 that is 180 days after the date of the enact-
11 ment of this Act, each large data holder shall—

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

17 (ii) make publicly available on the
18 website of the large data holder, in a clear
19 and conspicuous manner, a log that de-
20 scribes the date and nature of each mate-
21 rial change to the privacy policy of the
22 large data holder during the preceding 10-
23 year period in a manner that is sufficient
24 for a reasonable individual to understand
25 the effect of each material change.

1 (B) EXCLUSION.—This paragraph does not
2 apply to material changes to previous versions
3 of the privacy policy of a large data holder that
4 precede the date that is 180 days after the date
5 of the enactment of this Act.

6 (2) SHORT FORM NOTICE TO CONSUMERS.—

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

12 (i) is concise;

13 (ii) is clear and conspicuous;

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

22 (iv) includes an overview of individual
23 rights and disclosures to reasonably draw
24 attention to data practices that may be un-

1 expected or that involve sensitive covered
2 data; and

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

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

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

15 (a) ACCESS TO, AND CORRECTION, DELETION, AND
16 PORTABILITY OF, COVERED DATA.—After receiving a
17 verified request from an individual, including a parent act-
18 ing on behalf of a child of the parent, a covered entity
19 shall provide the individual with the right to—

20 (1) access—

21 (A) in a format that can be naturally read
22 by a human, the covered data of the individual
23 or child (as applicable) (or an accurate rep-
24 resentation of the covered data of the individual
25 or child (as applicable), if the covered data is

1 no longer in the possession of the covered entity
2 or a service provider acting on behalf of the
3 covered entity) that is collected, processed, or
4 retained by the covered entity or any service
5 provider of the covered entity;

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

11 (C) a description of the purpose for which
12 the covered entity transferred any covered data
13 of the individual or child (as applicable) to a
14 third party or service provider;

15 (2) correct any inaccuracy or incomplete infor-
16 mation with respect to the covered data of the indi-
17 vidual or child (as applicable) that is collected, proc-
18 essed, or retained by the covered entity and, for cov-
19 ered data that has been transferred, request the cov-
20 ered entity to notify any third party or service pro-
21 vider to which the covered entity transferred such
22 covered data of the corrected information, including
23 so that service providers may provide the assistance
24 required by section 111(a)(1)(C);

1 (3) delete covered data of the individual or child
2 (as applicable) that is retained by the covered entity
3 and, for covered data that has been transferred, re-
4 quest that the covered entity notify any third party
5 or service provider to which the covered entity trans-
6 ferred such covered data of the deletion request, in-
7 cluding so that service providers may provide the as-
8 sistance required by section 111(a)(1)(C);

9 (4) to the extent technically feasible, have ex-
10 ported covered data of the individual or child (as ap-
11 plicable) that is collected, processed, or retained by
12 the covered entity, without licensing restrictions that
13 unreasonably limit such transfers, in—

14 (A) a format that can be naturally read by
15 a human; and

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

18 (5) delete any content or information submitted
19 to the covered entity by the individual when a cov-
20 ered minor and, for any such content or information
21 that has been transferred, request that the covered
22 entity notify any third party or service provider to
23 which the covered entity transferred such content or
24 information of the deletion request, including so that

1 service providers may provide the assistance required
2 by section 111(a)(1)(C).

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

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

7 (2) with respect to—

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

13 (B) any instance beyond the first 3 in-
14 stances described in subparagraph (A), may
15 charge a reasonable fee for each additional re-
16 quest to exercise any such right during such
17 12-month period.

18 (c) TIMING.—

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

22 (A) by any covered entity that is a large
23 data holder or data broker, not later than 30
24 calendar days after receiving such request from

1 an individual, unless it is impossible or demon-
2 strably impracticable to verify the individual; or

3 (B) by a covered entity that is not a large
4 data holder or data broker, not later than 45
5 calendar days after receiving such request from
6 an individual, unless it is impossible or demon-
7 strably impracticable to verify the individual.

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

16 (d) VERIFICATION.—

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

20 (A) the individual whose covered data is
21 the subject of the request;

22 (B) the parent of the child whose covered
23 data (or, with respect to a request under sub-
24 section (a)(5), whose content or other informa-
25 tion) is the subject of the request; or

1 (C) another individual who is a natural
2 person who is authorized to make such a re-
3 quest on behalf of the individual whose covered
4 data is the subject of the request.

5 (2) ADDITIONAL INFORMATION.—If a covered
6 entity cannot make the verification described in
7 paragraph (1), the covered entity may request that
8 the individual making the request provide any addi-
9 tional information necessary for the sole purpose of
10 making such verification, except that—

11 (A) the request of the covered entity may
12 not be burdensome on the individual; and

13 (B) the covered entity may not process, re-
14 tain, or transfer such additional information for
15 any other purpose.

16 (e) EXCEPTIONS.—

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

21 (A) cannot reasonably make the
22 verification described in subsection (d)(1);

23 (B) determines that exercise of the right
24 would require access to, or the correction or de-
25 letion of, the sensitive covered data of an indi-

1 vidual other than the individual whose covered
2 data is the subject of the request;

3 (C) determines that exercise of the right
4 would require correction or deletion of covered
5 data subject to a warrant, lawfully executed
6 subpoena, or litigation hold notice or equivalent
7 preservation notice in connection with such war-
8 rant or subpoena or issued in a matter in which
9 the covered entity is a named party;

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

13 (E) determines that exercise of the right
14 would violate the professional ethical obligations
15 of the covered entity;

16 (F) reasonably believes that the request is
17 made to further fraud;

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

21 (H) reasonably believes that complying
22 with the request would threaten data security
23 or network security.

24 (2) PERMISSIVE EXCEPTIONS.—A covered enti-
25 ty may decline, in whole or in part, to comply with

1 a request to exercise a right described in subsection
2 (a), with adequate explanation to the individual
3 making the request, if compliance with the request
4 would—

5 (A) be demonstrably impracticable due to
6 technological limitations or prohibitive cost, and
7 if the covered entity provides a detailed descrip-
8 tion to the individual regarding the inability to
9 comply with the request due to technological
10 limitations or prohibitive cost;

11 (B) delete covered data necessary to per-
12 form a contract between the covered entity and
13 the individual;

14 (C) with respect to a right described in
15 paragraph (1) or (4) of subsection (a), require
16 the covered entity to release trade secrets or
17 other privileged, proprietary, or confidential
18 business information;

19 (D) prevent a covered entity from being
20 able to maintain a confidential record of opt-out
21 requests pursuant to this title that is main-
22 tained solely for the purpose of preventing cov-
23 ered data of an individual from being collected,
24 processed, retained, or transferred after the in-
25 dividual submits an opt-out request;

1 (E) with respect to a deletion request, re-
2 quire a private elementary or secondary school
3 (as determined under State law) or a private in-
4 stitution of higher education (as defined in title
5 I of the Higher Education Act of 1965 (20
6 U.S.C. 1001 et seq.)) to delete covered data, if
7 the deletion would unreasonably interfere with
8 the provision of education services by, or the or-
9 dinary operation of, the school or institution;

10 (F) delete covered data that relates to a
11 public figure regarding a matter of legitimate
12 public interest and for which the requesting in-
13 dividual has no reasonable expectation of pri-
14 vacy; or

15 (G) delete covered data that the covered
16 entity reasonably believes may be evidence of an
17 abuse of the products or services of the covered
18 entity, including a violation of terms of service.

19 (3) RULE OF CONSTRUCTION.—This section
20 may not be construed to require a covered entity or
21 service provider acting on behalf of a covered entity
22 to—

23 (A) retain covered data collected for a 1-
24 time transaction, if such covered data is not
25 processed or transferred by the covered entity

1 for any purpose other than completing such
2 transaction;

3 (B) re-identify, or attempt to re-identify,
4 de-identified data; or

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

8 (4) PARTIAL COMPLIANCE.—In the event a cov-
9 ered entity declines a request under paragraph (2),
10 the covered entity shall comply with the remainder
11 of the request if partial compliance is possible and
12 not unduly burdensome.

13 (5) NUMBER OF REQUESTS.—For purposes of
14 paragraph (2)(A), the receipt of a large number of
15 verified requests, on its own, may not be considered
16 to render compliance with a request demonstrably
17 impracticable.

18 (6) ADDITIONAL EXCEPTIONS.—

19 (A) IN GENERAL.—The Commission may
20 promulgate regulations, in accordance with sec-
21 tion 553 of title 5, United States Code, to es-
22 tablish additional permissive exceptions to sub-
23 section (a) necessary to protect the rights of in-
24 dividuals, to alleviate undue burdens on covered
25 entities, to prevent unjust or unreasonable out-

1 comes from the exercise of access, correction,
2 deletion, or portability rights, or to otherwise
3 fulfill the purposes of this section.

4 (B) CONSIDERATIONS.—In establishing
5 any exceptions under subparagraph (A), the
6 Commission shall consider any relevant changes
7 in technology, means for protecting privacy and
8 other rights, and beneficial uses of covered data
9 by covered entities.

10 (C) CLARIFICATION.—A covered entity
11 may decline to comply with a request of an in-
12 dividual to exercise a right under this section
13 pursuant to an exception the Commission estab-
14 lishes under this paragraph.

15 (f) LARGE DATA HOLDER METRICS REPORTING.—
16 With respect to each calendar year for which an entity
17 is a large data holder, such entity shall comply with the
18 following requirements:

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

21 (A) The number of verified access requests
22 under subsection (a)(1).

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

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

3 (D) The number of verified requests to opt
4 out of covered data transfers under section
5 106(a)(1).

6 (E) The number of verified requests to opt
7 out of targeted advertising under section
8 106(a)(2).

9 (F) For each category of request described
10 in subparagraphs (A) through (E), the number
11 of such requests that the large data holder com-
12 plied with in whole or in part.

13 (G) For each category of request described
14 in subparagraphs (A) through (E), the average
15 number of days within which the large data
16 holder substantively responded to the requests.

17 (2) PUBLIC DISCLOSURE.—Not later than July
18 1 of each calendar year, disclose the information
19 compiled under paragraph (1) for the previous cal-
20 endar year—

21 (A) in the privacy policy of the large data
22 holder; or

23 (B) on a publicly available website of the
24 large data holder that is accessible from a
25 hyperlink included in the privacy policy.

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

7 (h) ACCESSIBILITY.—

8 (1) LANGUAGE.—A covered entity shall facili-
9 tate the ability of individuals to make requests to ex-
10 ercise rights described in subsection (a) in any lan-
11 guage in which the covered entity provides a product
12 or service.

13 (2) INDIVIDUALS LIVING WITH DISABILITIES.—
14 The mechanisms by which a covered entity enables
15 individuals to make a request to exercise a right de-
16 scribed in subsection (a) shall be readily accessible
17 and usable by individuals living with disabilities.

18 **SEC. 106. OPT-OUT RIGHTS AND UNIVERSAL MECHANISMS.**

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

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

24 (A) shall provide an individual with a clear
25 and conspicuous means to opt out of the trans-

1 fer of the covered data of the individual to a
2 third party;

3 (B) upon establishment of an opt out
4 mechanism that meets the requirements and
5 technical specifications promulgated under sub-
6 section (b), shall allow an individual to make an
7 opt-out designation pursuant to subparagraph
8 (A) through the opt out mechanism;

9 (C) shall abide by an opt-out designation
10 made pursuant to subparagraph (A) and com-
11 municate such designation to all relevant serv-
12 ice providers and third parties; and

13 (D) except as provided in subsection (b) or
14 (c)(4) of section 102, paragraph (3) or (4) of
15 section 112(c), or section 120(b), need not
16 allow an individual to opt out of a transfer of
17 covered data made pursuant to a permissible
18 purpose described in paragraph (1), (2), (3),
19 (4), (5), (6), (7), (8), (9), (10), (11), (12),
20 (13), or (14) of section 102(d).

21 (2) RIGHT TO OPT OUT OF TARGETED ADVER-
22 TISING.—A covered entity that engages in targeted
23 advertising shall—

24 (A) provide an individual with a clear and
25 conspicuous means to opt out of the processing

1 and transfer of covered data of the individual in
2 furtherance of targeted advertising;

3 (B) upon establishment of an opt out
4 mechanism that meets the requirements and
5 technical specifications promulgated under sub-
6 section (b), allow an individual to make an opt-
7 out designation with respect to targeted adver-
8 tising through the opt-out mechanism; and

9 (C) abide by any such opt-out designation
10 made by an individual and communicate such
11 designation to all relevant service providers and
12 third parties.

13 (b) UNIVERSAL OPT-OUT MECHANISMS.—

14 (1) IN GENERAL.—Not later than 2 years after
15 the date of the enactment of this Act, the Commis-
16 sion shall, in consultation with the Secretary of
17 Commerce, promulgate regulations, in accordance
18 with section 553 of title 5, United States Code, to
19 establish requirements and technical specifications
20 for 1 or more opt-out mechanisms (including global
21 privacy signals, such as browser or device privacy
22 settings) for individuals to exercise the opt-out
23 rights established under this title through a single
24 interface that—

- 1 (A) ensures that the opt-out preference
2 signal—
- 3 (i) is clearly described, and easy-to-
4 use by a reasonable individual;
- 5 (ii) does not require that an individual
6 provide additional information beyond what
7 is necessary to indicate such preference;
- 8 (iii) clearly represents the preference
9 of an individual;
- 10 (iv) is provided—
- 11 (I) in the 10 most-used lan-
12 guages in which a covered entity pro-
13 vides products or services subject to
14 the opt-out; or
- 15 (II) if the covered entity provides
16 products or services subject to the
17 opt-out in fewer than 10 languages, in
18 the languages in which the covered
19 entity provides such products or serv-
20 ices; and
- 21 (v) is provided in a manner that is
22 reasonably accessible to and usable by indi-
23 viduals living with disabilities;
- 24 (B) provides a mechanism for an individual
25 to selectively opt out of the collection, proc-

1 essing, retention, or transfer of covered data by
2 a covered entity, without affecting the pref-
3 erences of the individual with respect to other
4 entities or disabling the opt-out preference sig-
5 nal globally;

6 (C) states that, in the case of a page or
7 setting view that the individual accesses to set
8 the opt-out preference signal, the individual
9 should see up to 2 choices, corresponding to the
10 rights established under subsection (a); and

11 (D) ensures that the opt-out preference
12 signal will be registered and set only by the in-
13 dividual or by another individual who is a nat-
14 ural person on behalf of the individual.

15 (2) EFFECT OF DESIGNATIONS.—A covered en-
16 tity shall abide by any designation made by an indi-
17 vidual through any mechanism that meets the re-
18 quirements and technical specifications promulgated
19 under paragraph (1).

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

21 (a) DARK PATTERNS PROHIBITED.—

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

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

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

3 (C) obtain, infer, or facilitate the consent
4 of an individual for any action that requires the
5 consent of an individual under this title.

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

10 (b) INDIVIDUAL AUTONOMY.—A covered entity may
11 not condition, effectively condition, attempt to condition,
12 or attempt to effectively condition the exercise of a right
13 described in this title through the use of any false, ficti-
14 tious, fraudulent, or materially misleading statement or
15 representation.

16 **SEC. 108. PROHIBITION ON DENIAL OF SERVICE AND WAIV-**
17 **ER OF RIGHTS.**

18 (a) RETALIATION THROUGH SERVICE OR PRICING
19 PROHIBITED.—A covered entity may not retaliate against
20 an individual for exercising any of the rights established
21 under this title, or any regulations promulgated under this
22 title, including by denying goods or services, charging dif-
23 ferent prices or rates for goods or services, or providing
24 a different level of quality of goods or services.

25 (b) RULES OF CONSTRUCTION.—

1 (1) BONA FIDE LOYALTY PROGRAMS.—

2 (A) IN GENERAL.—Nothing in subsection
3 (a) may be construed to prohibit a covered enti-
4 ty from offering—

5 (i) to an individual different prices,
6 rates, levels, qualities, or selections of
7 goods or services, or functionalities with
8 respect to a product or service, including
9 offering goods or services for no fee, if the
10 offering is in connection with the voluntary
11 participation of the individual in a bona
12 fide loyalty program, and if—

13 (I) the individual provided af-
14 firmative express consent to partici-
15 pate in such bona fide loyalty pro-
16 gram;

17 (II) the covered entity abides by
18 the exercise by the individual of any
19 right provided by subsection (b) or (c)
20 of section 102, section 105, or section
21 106; and

22 (III) the sale of covered data is
23 not a condition of participation in the
24 bona fide loyalty program; or

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

11 (B) BONA FIDE LOYALTY PROGRAM DE-
12 FINED.—For purposes of this section, the term
13 “bona fide loyalty program”—

14 (i) includes rewards, premium fea-
15 tures, discounts, and club card programs
16 offered by a covered entity; and

17 (ii) excludes such programs offered by
18 a covered high-impact social media com-
19 pany or 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 to
5 an individual, if any collection, processing, retention,
6 or transfer affected by the individual exercising a
7 right established under this title is necessary, pro-
8 portionate, and limited to providing such product or
9 service.

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

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

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

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

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

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

24 (A) the size and complexity of the covered
25 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 and, if such a report is reasonably credible, per-

1 forming a reasonable and timely investigation of
2 such report and taking appropriate action to protect
3 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(d) applies, except that retention
8 and disposal of biometric information shall be gov-
9 erned by section 102(c)(3). Such disposal shall in-
10 clude destroying, permanently erasing, or otherwise
11 modifying the covered data to make such data per-
12 manently unreadable or indecipherable and unre-
13 coverable to ensure ongoing compliance with this
14 section.

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

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

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

24 (c) REGULATIONS.—The Commission may, in con-
25 sultation with the Secretary of Commerce, promulgate, in

1 accordance with section 553 of title 5, United States Code,
2 technology-neutral, process-based regulations to carry out
3 this section.

4 **SEC. 110. EXECUTIVE RESPONSIBILITY.**

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

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

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

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

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

22 (b) REQUIREMENTS FOR LARGE DATA HOLDERS.—

23 (1) DESIGNATION.—A covered entity or service
24 provider that is a large data holder shall designate
25 1 qualified employee to serve as a privacy officer and

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 or other service provider and col-
9 lect, process, retain, or transfer covered data
10 only to the extent necessary, proportionate, and
11 limited to provide a service requested by the
12 covered entity or other service provider, as set
13 out in the contract described in paragraph (2);

14 (B) may not collect, process, retain, or
15 transfer covered data if the service provider has
16 actual knowledge that the covered entity or
17 other service provider violated this title with re-
18 spect to such data;

19 (C) shall assist the covered entity or other
20 service provider in fulfilling the obligations of
21 the covered entity or other service provider to
22 respond to consumer rights requests pursuant
23 to this title by—

24 (i) providing appropriate technical and
25 organizational support, taking into account
26 the nature of the processing and the infor-

1 mation reasonably available to the service
2 provider; or

3 (ii) fulfilling a request by the covered
4 entity or other service provider to execute
5 a consumer rights request that the covered
6 entity or other service provider has deter-
7 mined should be compiled with, by either—

8 (I) complying with the request
9 pursuant to the instructions of the
10 covered entity or other service pro-
11 vider; or

12 (II) providing written verification
13 to the covered entity or other service
14 provider that the service provider does
15 not hold data related to the request,
16 that complying with the request would
17 be inconsistent with the legal obliga-
18 tions of the service provider, or that
19 the request falls within an exception
20 pursuant to this title;

21 (D) shall, upon the reasonable request of
22 the covered entity or other service provider,
23 make available to the covered entity or other
24 service provider all information necessary to

1 demonstrate the compliance of the service pro-
2 vider with the requirements of this title;

3 (E) shall delete or return, as directed by
4 the covered entity or other service provider, all
5 covered data as soon as practicable after the
6 contractually agreed upon end of the provision
7 of services, unless the retention by the service
8 provider of covered data is required by law;

9 (F) may engage another service provider
10 for purposes of processing or retaining covered
11 data on behalf of the covered entity or other
12 service provider only after exercising reasonable
13 care in selecting another service provider as re-
14 quired by subsection (d), providing the covered
15 entity or other service provider with written no-
16 tice of the engagement, and entering into a
17 written contract that requires the other service
18 provider to satisfy the requirements of this title
19 with respect to covered data; and

20 (G) shall—

21 (i) allow and cooperate with reason-
22 able assessments by the covered entity or
23 other service provider at least annually; or

24 (ii) arrange for a qualified and inde-
25 pendent assessor to conduct an assessment

1 of the policies and technical and organiza-
2 tional measures of the service provider in
3 support of the obligations of the service
4 provider under this title at least annually,
5 using an appropriate and accepted control
6 standard or framework and assessment
7 procedure for such assessments, and report
8 the results of such assessment to the cov-
9 ered entity or other service provider.

10 (2) CONTRACT REQUIREMENTS.—An entity may
11 only operate as a service provider pursuant to a con-
12 tract between a covered entity and a service pro-
13 vider. Such contract—

14 (A) shall govern the data processing proce-
15 dures of the service provider with respect to any
16 collection, processing, retention, or transfer per-
17 formed on behalf of the covered entity;

18 (B) shall clearly set forth—

19 (i) instructions for collecting, proc-
20 essing, retaining, or transferring data;

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

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

1 (iv) the duration of the processing or
2 retention; and

3 (v) the rights and obligations of both
4 parties;

5 (C) may not relieve the covered entity or
6 service provider of any obligation under this
7 title; and

8 (D) shall prohibit—

9 (i) the collection, processing, reten-
10 tion, or transfer of covered data in a man-
11 ner that does not comply with the require-
12 ments of paragraph (1); and

13 (ii) combining covered data that the
14 service provider receives from or on behalf
15 of a covered entity with covered data that
16 the service provider receives from or on be-
17 half of another entity or collects from the
18 interaction of the service provider with an
19 individual, unless such combining is nec-
20 essary for a purpose described in section
21 102(d), other than a purpose described in
22 paragraph (7), (14), (15), or (16) of such
23 section, and is otherwise permitted under
24 the contract.

25 (b) THIRD PARTIES.—

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

4 (A) in the case of sensitive covered data—

5 (i) except as provided in clause (ii), a
6 purpose for which an individual gave af-
7 firmative express consent pursuant to sub-
8 section (b) or (c) of section 102; or

9 (ii) in the case of sensitive covered
10 data with respect to which affirmative ex-
11 press consent is not required pursuant to
12 subsection (b) of section 102, a purpose
13 for which the covered entity or service pro-
14 vider made a disclosure pursuant to section
15 104; or

16 (B) in the case of covered data that is not
17 sensitive covered data, a purpose for which the
18 covered entity or service provider made a disclo-
19 sure pursuant to section 104.

20 (2) CONTRACT REQUIREMENTS.—Before trans-
21 ferring covered data to a third party, a covered enti-
22 ty or service provider shall enter into a contract with
23 the third party that—

24 (A) identifies the purposes for which cov-
25 ered data is being transferred;

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

3 (C) with respect to the covered data trans-
4 ferred, requires the third party to comply with
5 all applicable provisions of, and regulations pro-
6 mulgated under, this title;

7 (D) requires the third party to notify the
8 covered entity or service provider if the third
9 party makes a determination that the third
10 party can no longer meet the obligations of the
11 third party under this title; and

12 (E) grants the covered entity or service
13 provider the right, upon notice (including under
14 subparagraph (D)), to take reasonable and ap-
15 propriate steps to stop and remediate unauthor-
16 ized use of covered data by the third party.

17 (c) RULES OF CONSTRUCTION.—

18 (1) SUCCESSIVE ACTOR VIOLATIONS.—

19 (A) IN GENERAL.—With respect to a viola-
20 tion of this title by a service provider or third
21 party regarding covered data received by the
22 service provider or third party from a covered
23 entity or another service provider, the covered
24 entity or service provider that transferred such
25 covered data may not be considered to be in

1 violation of this title if the covered entity or
2 service provider transferred the covered data in
3 compliance with the requirements of this title
4 and, at the time of transferring such covered
5 data, did not have actual knowledge, or reason
6 to believe, that the service provider or third
7 party to which the covered data was transferred
8 intended to violate this title.

9 (B) KNOWLEDGE OF VIOLATION.—A cov-
10 ered entity or service provider that transfers
11 covered data to a service provider or third party
12 and has actual knowledge, or reason to believe,
13 that such service provider or third party is vio-
14 lating, or is about to violate, the requirements
15 of this title shall immediately cease the transfer
16 of covered data to such service provider or third
17 party.

18 (2) PRIOR ACTOR VIOLATIONS.—An entity that
19 collects, processes, retains, or transfers covered data
20 in compliance with the requirements of this title may
21 not be considered to be in violation of this title as
22 a result of a violation by an entity from which it re-
23 ceives, or on whose behalf it collects, processes, re-
24 tains, or transfers, covered data.

25 (d) REASONABLE CARE.—

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

4 (2) TRANSFER TO THIRD PARTY.—A covered
5 entity or service provider shall exercise reasonable
6 care in deciding to transfer covered data to a third
7 party.

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

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

20 **SEC. 112. DATA BROKERS.**

21 (a) NOTICE.—A data broker shall—

22 (1) establish and maintain a publicly available
23 website; and

24 (2) place a clear and conspicuous, and not mis-
25 leading, notice on such publicly available website,

1 and any mobile application of the data broker,
2 that—

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

4 (B) states that an individual may exercise
5 a right described in section 105 or 106, and in-
6 cludes a link or other tool to allow an individual
7 to exercise such right;

8 (C) includes a link to the website described
9 in subsection (c)(3);

10 (D) is reasonably accessible to and usable
11 by individuals living with disabilities; and

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

14 (b) PROHIBITED PRACTICES.—A data broker may
15 not—

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

18 (A) stalking or harassing an individual; or

19 (B) engaging in fraud, identity theft, or
20 unfair or deceptive acts or practices; or

21 (2) misrepresent the business practices of the
22 data broker.

23 (c) DATA BROKER REGISTRATION.—

24 (1) IN GENERAL.—Not later than January 31
25 of each calendar year that follows a calendar year

1 during which an entity acted as a data broker with
2 respect to more than 5,000 individuals or devices
3 that identify or are linked or reasonably linkable to
4 an individual, such entity shall register with the
5 Commission in accordance with this subsection.

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

9 (A) Pay to the Commission a registration
10 fee of \$100.

11 (B) Provide the Commission with the fol-
12 lowing information:

13 (i) The legal name and primary valid
14 physical postal address, email address, and
15 internet address of the data broker.

16 (ii) A description of the categories of
17 covered data the data broker collects, proc-
18 esses, retains, or transfers.

19 (iii) The contact information of the
20 data broker, including the name of a con-
21 tact person, a human-monitored telephone
22 number, a human-monitored e-mail ad-
23 dress, a website, and a physical mailing ad-
24 dress.

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

4 (3) DATA BROKER REGISTRY.—

5 (A) ESTABLISHMENT.—The Commission
6 shall establish and maintain on a publicly avail-
7 able website a searchable list of data brokers
8 that are registered with the Commission under
9 this subsection.

10 (B) REQUIREMENTS.—The registry estab-
11 lished under subparagraph (A) shall—

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

14 (ii) include the information required
15 under paragraph (2)(B) for each data
16 broker;

17 (iii) include a mechanism by which an
18 individual, including a parent acting on be-
19 half of a child of the parent, may submit
20 to all registered data brokers a “Do Not
21 Collect” request that results in registered
22 data brokers no longer collecting covered
23 data related to such individual or child (as
24 applicable) without the affirmative express
25 consent of such individual; and

1 (iv) include a mechanism by which an
2 individual, including a parent acting on be-
3 half of a child of the parent, may submit
4 to all registered data brokers a “Delete My
5 Data” request that results in registered
6 data brokers deleting all covered data re-
7 lated to such individual or child (as appli-
8 cable) that the data broker did not collect
9 directly from such individual or when act-
10 ing as a service provider.

11 (C) AFFORDABILITY.—A data broker may
12 not charge an individual a fee to exercise a
13 right under this paragraph.

14 (4) DO NOT COLLECT AND DELETE MY DATA
15 REQUESTS.—

16 (A) COMPLIANCE.—Subject to subpara-
17 graph (B), each data broker that receives a re-
18 quest from an individual, including a parent
19 acting on behalf of a child of the parent, using
20 the mechanism established under paragraph
21 (3)(B)(iii) or paragraph (3)(B)(iv) shall comply
22 with such request not later than 30 days after
23 the date on which the request is received by the
24 data broker.

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

3 (i) the data broker has actual knowl-
4 edge that the individual has been convicted
5 of a crime related to the abduction or sex-
6 ual exploitation of a child; and

7 (ii) the data collected by the data
8 broker is necessary—

9 (I) to carry out a national or
10 State-run sex offender registry; or

11 (II) for the National Center for
12 Missing and Exploited Children.

13 **SEC. 113. COMMISSION-APPROVED COMPLIANCE GUIDE-**
14 **LINES.**

15 (a) APPLICATION FOR COMPLIANCE GUIDELINE AP-
16 PROVAL.—

17 (1) IN GENERAL.—A covered entity that is not
18 a data broker and is not a large data holder, or a
19 group of such covered entities, may apply to the
20 Commission for approval of 1 or more sets of com-
21 pliance guidelines governing the collection, proc-
22 essing, retention, or transfer of covered data by the
23 covered entity or covered entities.

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

1 (A) a description of how the proposed
2 guidelines will meet or exceed the applicable re-
3 quirements of this title;

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

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

10 (D) a description of an independent orga-
11 nization, not associated with any of the in-
12 tended adhering covered entities, that will ad-
13 minister the proposed guidelines; and

14 (E) a description of how such intended ad-
15 hering entities will be assessed for adherence to
16 the proposed guidelines by the independent or-
17 ganization described in subparagraph (D).

18 (3) COMMISSION REVIEW.—

19 (A) INITIAL APPROVAL.—

20 (i) PUBLIC COMMENT PERIOD.—Not
21 later than 90 days after receipt of an ap-
22 plication regarding proposed guidelines
23 submitted pursuant to paragraph (1), the
24 Commission shall publish the application

1 and provide an opportunity for public com-
2 ment on such proposed guidelines.

3 (ii) APPROVAL CRITERIA.—The Com-
4 mission shall approve an application re-
5 garding proposed guidelines submitted pur-
6 suant to paragraph (1), including the inde-
7 pendent organization that will administer
8 the guidelines, if the applicant dem-
9 onstrates that the proposed guidelines—

10 (I) meet or exceed the applicable
11 requirements of this title;

12 (II) provide for regular review
13 and validation by an independent or-
14 ganization to ensure that the covered
15 entity or covered entities adhering to
16 the guidelines continue to meet or ex-
17 ceed the applicable requirements of
18 this title; and

19 (III) include a means of enforce-
20 ment if a covered entity does not meet
21 or exceed the requirements in the
22 guidelines, which may include referral
23 to the Commission for enforcement
24 under section 115 or referral to the

1 appropriate State attorney general for
2 enforcement under section 116.

3 (iii) **TIMELINE.**—Not later than 1
4 year after the date on which the Commis-
5 sion receives an application regarding pro-
6 posed guidelines pursuant to paragraph
7 (1), the Commission shall issue a deter-
8 mination approving or denying the applica-
9 tion, including the relevant independent or-
10 ganization, and providing the reasons for
11 approving or denying the application.

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

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

23 (ii) **TIMELINE.**—The Commission
24 shall approve or deny any significant
25 change to guidelines submitted under

1 clause (i) not later than 180 days after the
2 date on which the Commission receives the
3 submission for approval.

4 (b) WITHDRAWAL OF APPROVAL.—

5 (1) IN GENERAL.—If at any time the Commis-
6 sion determines that guidelines previously approved
7 under this section no longer meet the applicable re-
8 quirements of this title or that compliance with the
9 approved guidelines is insufficiently enforced by the
10 independent organization administering the guide-
11 lines, the Commission shall notify the relevant cov-
12 ered entity or group of covered entities and the inde-
13 pendent organization of the determination of the
14 Commission to withdraw approval of the guidelines,
15 including the basis for the determination.

16 (2) OPPORTUNITY TO CURE.—

17 (A) IN GENERAL.—Not later than 180
18 days after receipt of a notice under paragraph
19 (1), the covered entity or group of covered enti-
20 ties and the independent organization may cure
21 any alleged deficiency with the guidelines or the
22 enforcement of the guidelines and submit each
23 proposed cure to the Commission.

24 (B) EFFECT ON WITHDRAWAL OF AP-
25 PROVAL.—If the Commission determines that

1 cures proposed under subparagraph (A) elimi-
2 nate alleged deficiencies in the guidelines, the
3 Commission may not withdraw the approval of
4 such guidelines on the basis of such defi-
5 ciencies.

6 (c) CERTIFICATION.—A covered entity with guide-
7 lines approved by the Commission under this section
8 shall—

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

11 (2) as part of the self-certification under para-
12 graph (1), indicate the independent organization re-
13 sponsible for assessing compliance with the guide-
14 lines.

15 (d) REBUTTABLE PRESUMPTION OF COMPLIANCE.—
16 A covered entity that is eligible to participate in guidelines
17 approved under this section, participates in the guidelines,
18 and is in compliance with the guidelines shall be entitled
19 to a rebuttable presumption that the covered entity is in
20 compliance with the relevant provisions of this title to
21 which the guidelines apply.

22 (e) ELIGIBILITY OF SERVICE PROVIDERS.—This sec-
23 tion shall apply to a service provider that is not a large
24 data holder, or a group of such service providers, in the
25 same manner as this section applies to a covered entity

1 or group of covered entities. Such a service provider or
2 group of service providers may apply for approval of, and
3 participate in, the same guidelines as a covered entity or
4 group of covered entities.

5 **SEC. 114. PRIVACY-ENHANCING TECHNOLOGY PILOT PRO-**
6 **GRAM.**

7 (a) **PRIVACY-ENHANCING TECHNOLOGY DEFINED.**—
8 In this section, the term “privacy-enhancing tech-
9 nology”—

10 (1) means any software or hardware solution,
11 cryptographic algorithm, or other technical process
12 of extracting the value of information without sub-
13 stantially reducing the privacy and security of the
14 information; and

15 (2) includes technologies with functionality
16 similar to homomorphic encryption, differential pri-
17 vacy, zero-knowledge proofs, synthetic data genera-
18 tion, federated learning, and secure multi-party com-
19 putation.

20 (b) **ESTABLISHMENT.**—Not later than 1 year after
21 the date of the enactment of this Act, the Commission
22 shall establish and carry out a pilot program to encourage
23 private sector use of privacy-enhancing technologies for
24 the purposes of protecting covered data to comply with
25 section 109.

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

3 (1) develop and implement a petition process
4 for covered entities to request to be a part of the
5 pilot program; and

6 (2) build an auditing system that leverages pri-
7 vacy-enhancing technologies to support the enforce-
8 ment actions of the Commission.

9 (d) PETITION PROCESS.—A covered entity wishing to
10 be accepted into the pilot program established under sub-
11 section (b) shall demonstrate to the Commission that the
12 privacy-enhancing technologies to be used under the pilot
13 program by the covered entity will establish data security
14 practices that meet or exceed all or some of the require-
15 ments in section 109. If the covered entity demonstrates
16 the privacy-enhancing technologies meet or exceed the re-
17 quirements in section 109, the Commission may accept the
18 covered entity to be a part of the pilot program. If the
19 Commission does not accept a covered entity to be a part
20 of the pilot program, the Commission shall provide an ade-
21 quate response to the covered entity detailing why the cov-
22 ered entity was not accepted, and the covered entity may
23 subsequently revise the petition of the covered entity to
24 address any deficiencies indicated by the Commission in
25 the response of the Commission to the covered entity.

1 (e) REQUIREMENTS.—In carrying out the pilot pro-
2 gram established under subsection (b), the Commission
3 shall—

4 (1) receive input from private, public, and aca-
5 demic stakeholders; and

6 (2) develop ongoing public and private sector
7 engagement, in consultation with the Secretary of
8 Commerce, to disseminate voluntary, consensus-
9 based resources to increase the integration of pri-
10 vacy-enhancing technologies in data collection, shar-
11 ing, and analytics by the public and private sectors.

12 (f) CONCLUSION OF PILOT PROGRAM.—The Commis-
13 sion shall terminate the pilot program established under
14 subsection (b) not later than 10 years after the commence-
15 ment of the program.

16 (g) STUDY REQUIRED.—

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

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

21 (B) to determine the effectiveness of using
22 privacy-enhancing technologies at the Commis-
23 sion to support oversight of the data security
24 practices of covered entities; and

1 (C) to develop recommendations to improve
2 and advance privacy-enhancing technologies, in-
3 cluding by improving communication and co-
4 ordination between covered entities and the
5 Commission to increase implementation of pri-
6 vacy-enhancing technologies by such entities
7 and the Commission.

8 (2) INITIAL BRIEFING.—Not later than 3 years
9 after the date of the enactment of this Act, the
10 Comptroller General shall brief the Committee on
11 Energy and Commerce of the House of Representa-
12 tives and the Committee on Commerce, Science, and
13 Transportation of the Senate on the initial results of
14 the study conducted under paragraph (1).

15 (3) FINAL REPORT.—Not later than 240 days
16 after the date on which the briefing required by
17 paragraph (2) is conducted, the Comptroller General
18 shall submit to the Committee on Energy and Com-
19 merce of the House of Representatives and the Com-
20 mittee on Commerce, Science, and Transportation of
21 the Senate a final report setting forth the results of
22 the study conducted under paragraph (1), including
23 the recommendations developed under subparagraph
24 (C) of such paragraph.

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

7 (i) WITHDRAWAL FROM THE PILOT PROGRAM.—If at
8 any time the Commission determines that a covered entity
9 accepted to be a part of the pilot program established
10 under subsection (b) is no longer maintaining the use of
11 privacy-enhancing technologies, the Commission shall no-
12 tify the covered entity of the determination of the Commis-
13 sion to withdraw approval for the covered entity to be a
14 part of the pilot program and the basis for doing so. Not
15 later than 180 days after the date on which a covered enti-
16 ty receives such notice, the covered entity may cure any
17 alleged deficiency with the use of privacy-enhancing tech-
18 nologies and submit each proposed cure to the Commis-
19 sion. If the Commission determines that such cures elimi-
20 nate alleged deficiencies with the use of privacy-enhancing
21 technologies, the Commission may not withdraw the ap-
22 proval of the covered entity to be a part of the pilot pro-
23 gram on the basis of such deficiencies.

24 (j) LIMITATIONS ON LIABILITY.—Any covered entity
25 that petitions, and is accepted, to be part of the pilot pro-

1 gram established under subsection (b), actively imple-
2 ments and maintains the use of privacy-enhancing tech-
3 nologies, and is determined by the Commission to be in
4 compliance with the program shall—

5 (1) for any action under section 115 or 116 for
6 a violation of section 109, be deemed to be in com-
7 pliance with section 109 with respect to the covered
8 data subject to the privacy-enhancing technologies;
9 and

10 (2) for any action under section 117 for a viola-
11 tion of section 109, be entitled to a rebuttable pre-
12 sumption that such entity is in compliance with sec-
13 tion 109 with respect to the covered data subject to
14 the privacy-enhancing technologies.

15 **SEC. 115. ENFORCEMENT BY FEDERAL TRADE COMMIS-**
16 **SION.**

17 (a) NEW BUREAU.—

18 (1) IN GENERAL.—Subject to the availability of
19 appropriations, the Commission shall establish, with-
20 in the Commission, a new bureau comparable in
21 structure, size, organization, and authority to the ex-
22 isting bureaus within the Commission related to con-
23 sumer protection and competition.

24 (2) MISSION.—The mission of the bureau es-
25 tablished under this subsection shall be to assist the

1 Commission in exercising the authority of the Com-
2 mission under this title and related authorities.

3 (3) STAFF.—

4 (A) IN GENERAL.—In staffing the bureau
5 established under this subsection, the Commis-
6 sion shall ensure the allocation of full time em-
7 ployees or full time employee equivalents that
8 include attorneys, economists, investigators,
9 technologists, and mental health professionals
10 with experience in the well-being of children
11 and teens.

12 (B) TECHNOLOGIST DEFINED.—For the
13 purposes of this paragraph, the term “tech-
14 nologist” means an individual with training and
15 expertise with respect to technology, including
16 state-of-the art information technology, network
17 or data security, hardware or software develop-
18 ment, privacy-enhancing technologies, cryptog-
19 raphy, computer science, data science, adver-
20 tising technology, web tracking, machine learn-
21 ing, and other related fields and applications.

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

1 (b) ENFORCEMENT BY COMMISSION.—

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

9 (2) POWERS OF COMMISSION.—

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

20 (B) PRIVILEGES AND IMMUNITIES.—Any
21 entity that violates this title or a regulation
22 promulgated under this title shall be subject to
23 the penalties and entitled to the privileges and
24 immunities provided in the Federal Trade Com-
25 mission Act (15 U.S.C. 41 et seq.).

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

9 (A) common carriers subject to title II of
10 the Communications Act of 1934 (47 U.S.C.
11 201 et seq.); and

12 (B) organizations not organized to carry
13 on business for their own profit or that of their
14 members.

15 (4) PENALTY OFFSET FOR STATE OR INDI-
16 VIDUAL ACTIONS.—Any amount that a court orders
17 an entity to pay in an action brought under this sub-
18 section shall be offset by any amount a court has or-
19 dered the entity to pay in an action brought against
20 the entity for the same violation under section 116
21 or 117.

22 (5) PRIVACY AND SECURITY VICTIMS RELIEF
23 FUND.—

24 (A) ESTABLISHMENT OF VICTIMS RELIEF
25 FUND.—There is established in the Treasury of

1 the United States a separate fund to be known
2 as the “Privacy and Security Victims Relief
3 Fund” (in this paragraph referred to as the
4 “Victims Relief Fund”).

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

13 (C) USE OF FUND AMOUNTS.—

14 (i) AVAILABILITY TO THE COMMIS-
15 SION.—Notwithstanding section 3302 of
16 title 31, United States Code, amounts in
17 the Victims Relief Fund shall be available
18 to the Commission, without fiscal year lim-
19 itation, to provide redress, damages, pay-
20 ments or compensation, or other monetary
21 relief to persons affected by an act or prac-
22 tice for which civil penalties, other mone-
23 tary relief, or any other forms of relief (in-
24 cluding injunctive relief) have been ordered
25 in a civil action or administrative pro-

1 ceeding the Commission commences, or in
2 any civil action the Attorney General of the
3 United States commences on behalf of the
4 Commission, to enforce this title or a regu-
5 lation promulgated under this title.

6 (ii) OTHER PERMISSIBLE USES.—To
7 the extent that individuals cannot be lo-
8 cated or such redress, damages, payments
9 or compensation, or other monetary relief
10 are otherwise not practicable, the Commis-
11 sion may use amounts in the Victims Re-
12 lief Fund for the purpose of—

13 (I) consumer or business edu-
14 cation relating to data privacy or data
15 security; or

16 (II) engaging in technological re-
17 search that the Commission considers
18 necessary to implement this title, in-
19 cluding promoting privacy-enhancing
20 technologies that promote compliance
21 with this title.

22 (D) CALCULATION.—Any amount that the
23 Commission provides to a person as redress,
24 payments or compensation, or other monetary
25 relief under subparagraph (C) with respect to a

1 violation by an entity shall be offset by any
2 amount the person received from an action
3 brought against the entity for the same viola-
4 tion under section 116 or 117.

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

12 (c) REPORT.—

13 (1) IN GENERAL.—Not later than 4 years after
14 the date of the enactment of this Act, and annually
15 thereafter, the Commission shall submit to Congress
16 a report describing investigations conducted during
17 the prior year with respect to violations of this title,
18 including—

19 (A) the number of such investigations the
20 Commission commenced;

21 (B) the number of such investigations the
22 Commission closed with no official agency ac-
23 tion;

1 (C) the disposition of such investigations,
2 if such investigations have concluded and re-
3 sulted in official agency action; and

4 (D) for each investigation that was closed
5 with no official agency action, the industry sec-
6 tors of the covered entities subject to each in-
7 vestigation.

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

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

18 (A) the policy priorities of the Commission
19 and any changes to the previous policy prior-
20 ities of the Commission;

21 (B) any rulemaking proceedings projected
22 to be commenced, including any such pro-
23 ceedings to amend or repeal a rule;

1 (C) any plans to develop, update, or with-
2 draw guidelines or guidance required under this
3 title;

4 (D) any plans to restructure the Commis-
5 sion; and

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

10 **SEC. 116. ENFORCEMENT BY STATES.**

11 (a) CIVIL ACTION.—

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

1 half of the residents of the State, in an appropriate
2 Federal district court of the United States to—

3 (A) enjoin such act or practice;

4 (B) enforce compliance with this title or
5 the regulations promulgated under this title;

6 (C) obtain civil penalties;

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

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

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

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

24 (b) RIGHTS OF THE COMMISSION.—

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

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

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

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

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

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

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

13 (e) VENUE; SERVICE OF PROCESS.—

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

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

22 (A) is an inhabitant; or

23 (B) may be found.

24 (f) GAO STUDY.—

1 (1) IN GENERAL.—The Comptroller General of
2 the United States shall conduct a study of the prac-
3 tice of State attorneys general hiring, or otherwise
4 contracting with, outside firms to assist in enforce-
5 ment efforts pursuant to this title, which shall in-
6 clude the study of—

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

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

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

15 (D) the bid and selection process for such
16 outside firms, including reviews of conflicts of
17 interest;

18 (E) the practices State attorneys general
19 set in place to protect sensitive information that
20 would become accessible by outside firms while
21 the outside firms are assisting in such enforce-
22 ment efforts;

23 (F) the percentage of monetary recovery
24 that is returned to victims and the percentage

1 of such recovery that is retained by outside
2 firms; and

3 (G) the market average for the hourly rate
4 of hired or contracted attorneys in each market.

5 (2) REPORT.—Not later than 1 year after the
6 date of the enactment of this Act, the Comptroller
7 General shall submit to the Committee on Energy
8 and Commerce of the House of Representatives and
9 the Committee on Commerce, Science, and Trans-
10 portation of the Senate a report on the results of the
11 study conducted under paragraph (1).

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

19 (1) bring an action or other regulatory pro-
20 ceeding arising solely under the laws in effect in
21 such State; or

22 (2) exercise the powers conferred on the attor-
23 ney general, chief consumer protection officer, or of-
24 ficer or office by the laws of such State, including
25 the ability to conduct investigations, to administer

1 oaths or affirmations, or to compel the attendance of
2 witnesses or the production of documentary or other
3 evidence.

4 (h) CALCULATION.—Any amount that a court orders
5 an entity to pay to a person under this section shall be
6 offset by any amount the person received from an action
7 brought against the entity for the same violation under
8 section 115 or 117.

9 **SEC. 117. ENFORCEMENT BY PERSONS.**

10 (a) CIVIL ACTION.—

11 (1) IN GENERAL.—Subject to subsections (b)
12 and (c), a person may bring a civil action against a
13 covered entity or service provider for a violation of
14 subsection (b) or (c) of section 102, subsection (a)
15 or (e) of section 104, section 105, subsection (a) or
16 (b)(2) of section 106, section 107, section 108, sec-
17 tion 109 to the extent such action alleges a data
18 breach arising from a violation of subsection (a) of
19 such section, subsection (d) of section 111, or sub-
20 section (c)(4) of section 112, or a regulation promul-
21 gated thereunder, in an appropriate Federal district
22 court of the United States.

23 (2) RELIEF.—

24 (A) IN GENERAL.—In a civil action
25 brought under paragraph (1) in which the

1 plaintiff prevails, the court may award the
2 plaintiff—

3 (i) an amount equal to the sum of any
4 actual damages;

5 (ii) injunctive relief, including an
6 order that an entity retrieve any covered
7 data transferred in violation of this title;

8 (iii) declaratory relief; and

9 (iv) reasonable attorney fees and liti-
10 gation costs.

11 (B) BIOMETRIC AND GENETIC INFORMA-
12 TION.—In a civil action brought under para-
13 graph (1) for a violation of this title with re-
14 spect to section 102(c), in which the plaintiff
15 prevails, if the conduct underlying the violation
16 occurred primarily and substantially in Illinois,
17 the court may award the plaintiff—

18 (i) for a violation involving biometric
19 information, the same relief as set forth in
20 section 20 of the Biometric Information
21 Privacy Act (740 ILCS 14/20), as such
22 statute reads on December 31, 2024; or

23 (ii) for a violation involving genetic in-
24 formation, the same relief as set forth in
25 section 40 of the Genetic Information Pri-

1 vacy Act (410 ILCS 513/40), as such stat-
2 ute reads on December 31, 2024.

3 (C) DATA SECURITY.—

4 (i) IN GENERAL.—In a civil action
5 brought under paragraph (1) for a viola-
6 tion of this title alleging unauthorized ac-
7 cess of covered information as a result of
8 a violation of section 109(a), in which the
9 plaintiff prevails, the court may award a
10 plaintiff who is a resident of California the
11 same relief as set forth in section
12 1798.150 of the California Civil Code, as
13 such statute read on January 1, 2024.

14 (ii) COVERED INFORMATION DE-
15 FINED.—For purposes of this subpara-
16 graph, the term “covered information”
17 means the following:

18 (I) A username, email address, or
19 telephone number of an individual in
20 combination with a password or secu-
21 rity question or answer that would
22 permit access to an account held by
23 the individual that contains or pro-
24 vides access to sensitive covered data.

1 (II) The first name or first initial
2 of an individual and the last name of
3 the individual in combination with 1
4 or more of the following categories of
5 sensitive covered data, if either the
6 name or the sensitive covered data are
7 not encrypted or redacted:

8 (aa) A government-issued
9 identifier described in section
10 101(49)(A)(i).

11 (bb) A financial account
12 number described in section
13 101(49)(A)(iv).

14 (cc) Health information, but
15 only to the extent such informa-
16 tion reveals the history of med-
17 ical treatment or diagnosis by a
18 health care professional of the in-
19 dividual.

20 (dd) Biometric information.

21 (ee) Genetic information.

22 (D) LIMITATIONS ON DUAL ACTIONS.—

23 Any amount that a court orders an entity to
24 pay to a person under subparagraph (A)(i),
25 (B), or (C) shall be offset by any amount the

1 person received from an action brought against
2 the entity for the same violation under section
3 115 or 116.

4 (b) OPPORTUNITY TO CURE IN ACTIONS FOR IN-
5 JUNCTIVE RELIEF.—

6 (1) NOTICE.—Subject to paragraph (3), an ac-
7 tion for injunctive relief may be brought by a person
8 under this section only if, prior to initiating such ac-
9 tion against an entity, the person provides to the en-
10 tity written notice identifying the specific provisions
11 of this title the person alleges have been or are being
12 violated.

13 (2) EFFECT OF CURE.—In the event a cure is
14 possible with respect to a violation alleged in a no-
15 tice described in paragraph (1) and, not later than
16 60 days after the date of receipt of such notice, the
17 entity cures such violation and provides the person
18 an express written statement that the violation has
19 been cured and that no further such violations shall
20 occur, an action for injunctive relief may not be per-
21 mitted with respect to the noticed violation.

22 (3) INJUNCTIVE RELIEF FOR A SUBSTANTIAL
23 PRIVACY HARM.—Notice is not required under para-
24 graph (1) prior to bringing an action for injunctive

1 relief for a violation that resulted in a substantial
2 privacy harm.

3 (c) NOTICE OF ACTIONS SEEKING ACTUAL DAM-
4 AGES.—

5 (1) NOTICE.—Subject to paragraph (4), an ac-
6 tion under this section for actual damages may be
7 brought by a person only if, 60 days prior to initi-
8 ating such action against an entity, the person pro-
9 vides the entity written notice identifying the specific
10 provisions of this title the person alleges have been
11 or are being violated.

12 (2) SETTLEMENT.—An entity that receives a
13 written notice from a person under paragraph (1)
14 may settle with the person who sent the written no-
15 tice.

16 (3) EFFECT OF SETTLEMENT.—In the event of
17 a settlement under paragraph (2), the terms of such
18 settlement shall govern any future action under this
19 section for actual damages between the parties to
20 the settlement that relates to the underlying facts
21 that resulted in the settlement.

22 (4) NO NOTICE REQUIRED FOR A SUBSTANTIAL
23 PRIVACY HARM.—Notice is not required under para-
24 graph (1) prior to bringing an action for actual
25 damages for a violation of this title that resulted in

1 a substantial privacy harm, if such action includes a
2 claim for a preliminary injunction or temporary re-
3 straining order.

4 (d) PRE-DISPUTE ARBITRATION AGREEMENTS.—

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

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

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

14 (2) DETERMINATION OF APPLICABILITY.—Any
15 issue as to whether this subsection applies to a dis-
16 pute shall be determined under Federal law. The ap-
17 plicability of this subsection to an agreement to arbi-
18 trate and the validity and enforceability of an agree-
19 ment to which this subsection applies shall be deter-
20 mined by a Federal court, rather than an arbitrator,
21 irrespective of whether the party resisting arbitra-
22 tion challenges the arbitration agreement specifically
23 or in conjunction with other terms of the contract
24 containing the agreement, and irrespective of wheth-

1 er the agreement purports to delegate the deter-
2 mination to an arbitrator.

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

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

12 (f) BAD FAITH.—If a person represented by counsel
13 brings a civil action under this section against a covered
14 entity or service provider requesting actual damages from
15 the covered entity or service provider, and fails to provide
16 notice to the covered entity or service provider in accord-
17 ance with this section, the action may be dismissed with-
18 out prejudice and may not be reinstated until the person
19 has complied with the notice requirements of this section.

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

21 (a) PREEMPTION OF STATE LAWS.—

22 (1) CONGRESSIONAL INTENT.—The purposes of
23 this section are to—

24 (A) establish a uniform national privacy
25 and data security standard in the United States

1 to prevent administrative costs and burdens
2 from being placed on interstate commerce; and

3 (B) expressly preempt the laws of a State
4 or political subdivision of a State as provided in
5 this subsection.

6 (2) PREEMPTION.—Except as provided in para-
7 graphs (3) and (4), no State or political subdivision
8 of a State may adopt, maintain, enforce, impose, or
9 continue in effect any law, regulation, rule, require-
10 ment, prohibition, standard, or other provision cov-
11 ered by the provisions of this title or a rule, regula-
12 tion, or requirement promulgated under this title.

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

17 (A) Consumer protection laws of general
18 applicability, such as laws regulating deceptive,
19 unfair, or unconscionable practices.

20 (B) Civil rights laws.

21 (C) Provisions of laws that address the pri-
22 vacy rights or other protections of employees or
23 employee information.

1 (D) Provisions of laws that address the
2 privacy rights or other protections of students
3 or student information.

4 (E) Provisions of laws, insofar as such pro-
5 visions address notification requirements in the
6 event of a data breach.

7 (F) Contract or tort law.

8 (G) Criminal laws.

9 (H) Civil laws regarding—

10 (i) blackmail;

11 (ii) stalking (including cyberstalking);

12 (iii) cyberbullying;

13 (iv) intimate images (whether authen-
14 tic or computer-generated) known to be
15 nonconsensual;

16 (v) child abuse;

17 (vi) child sexual abuse material;

18 (vii) child abduction or attempted
19 child abduction;

20 (viii) child trafficking; or

21 (ix) sexual harassment.

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

1 (J) Provisions of laws that address public
2 records, criminal justice information systems,
3 arrest records, mug shots, conviction records, or
4 non-conviction records.

5 (K) Provisions of laws that address bank-
6 ing records, financial records, tax records, So-
7 cial Security numbers, credit cards, identity
8 theft, credit reporting and investigations, credit
9 repair, credit clinics, or check-cashing services.

10 (L) Provisions of laws that address elec-
11 tronic surveillance, wiretapping, or telephone
12 monitoring.

13 (M) Provisions of laws that address unso-
14 licited email messages, telephone solicitation, or
15 caller identification.

16 (N) Provisions of laws that protect the pri-
17 vacy of health information, healthcare informa-
18 tion, medical information, medical records, HIV
19 status, or HIV testing.

20 (O) Provisions of laws that address the
21 confidentiality of library records.

22 (P) Provisions of laws that address the use
23 of encryption as a means of providing data se-
24 curity.

1 (4) ADDITIONAL PREEMPTION LIMITATIONS.—

2 Notwithstanding paragraph (2), the provisions of
3 this title shall preempt any State law, rule, or regu-
4 lation that provides protections for children or teens
5 only to the extent that such State law, rule, or regu-
6 lation conflicts with a provision of this title. Nothing
7 in this title shall be construed to prohibit any State
8 from enacting a law, rule, or regulation that pro-
9 vides greater protection to children or teens than the
10 provisions of this title.

11 (b) FEDERAL LAW PRESERVATION.—

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

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

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

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

25 (2) ANTITRUST SAVINGS CLAUSE.—

1 (A) ANTITRUST LAWS DEFINED.—For pur-
2 poses of this paragraph, the term “antitrust
3 laws”—

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

7 (ii) includes section 5 of the Federal
8 Trade Commission Act (15 U.S.C. 45), to
9 the extent such section applies to unfair
10 methods of competition.

11 (B) FULL APPLICATION OF THE ANTI-
12 TRUST LAWS.—Nothing in this title or a regula-
13 tion promulgated under this title may be con-
14 strued to modify, impair, supersede the oper-
15 ation of, or preclude the application of the anti-
16 trust laws.

17 (3) APPLICATION OF OTHER FEDERAL PRIVACY
18 AND DATA SECURITY REQUIREMENTS.—

19 (A) IN GENERAL.—To the extent that a
20 covered entity or service provider is required to
21 comply with any Federal law or regulation de-
22 scribed in subparagraph (B), such covered enti-
23 ty or service provider is not subject to this title
24 with respect to the activities governed by the re-
25 quirements of such law or regulation.

1 (B) LAWS AND REGULATIONS DE-
2 SCRIBED.—The Federal laws and regulations
3 described in this subparagraph are the fol-
4 lowing:

5 (i) Title V of the Gramm-Leach-Bliley
6 Act (15 U.S.C. 6801 et seq.).

7 (ii) Part C of title XI of the Social
8 Security Act (42 U.S.C. 1320d et seq.).

9 (iii) Subtitle D of the Health Informa-
10 tion Technology for Economic and Clinical
11 Health Act (42 U.S.C. 17921 et seq.).

12 (iv) The regulations promulgated pur-
13 suant to section 264(c) of the Health In-
14 surance Portability and Accountability Act
15 of 1996 (42 U.S.C. 1320d–2 note).

16 (v) The requirements regarding the
17 confidentiality of substance use disorder
18 information under section 543 of the Pub-
19 lic Health Service Act (42 U.S.C. 290dd–
20 2) or any regulation promulgated under
21 such section.

22 (vi) The Fair Credit Reporting Act
23 (15 U.S.C. 1681 et seq.).

24 (vii) Section 444 of the General Edu-
25 cation Provisions Act (commonly known as

1 the “Family Educational Rights and Pri-
2 vacy Act of 1974”) (20 U.S.C. 1232g) and
3 part 99 of title 34, Code of Federal Regu-
4 lations (or any successor regulation), to
5 the extent a covered entity or service pro-
6 vider is an educational agency or institu-
7 tion (as defined in such section or section
8 99.3 of title 34, Code of Federal Regula-
9 tions (or any successor regulation)).

10 (viii) The regulations related to the
11 protection of human subjects under part
12 46 of title 45, Code of Federal Regula-
13 tions.

14 (x) The Health Care Quality Improve-
15 ment Act of 1986 (42 U.S.C. 11101 et
16 seq.).

17 (xi) Part C of title IX of the Public
18 Health Service Act (42 U.S.C. 299b–21 et
19 seq.).

20 (xii) Chapter 123 of title 18, United
21 States Code.

22 (C) IMPLEMENTATION GUIDANCE.—Not
23 later than 1 year after the date of the enact-
24 ment of this Act, the Commission shall issue

1 guidance with respect to the implementation of
2 this paragraph.

3 (c) PRESERVATION OF COMMON LAW OR STATUTORY
4 CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this
5 title, nor any amendment, standard, rule, requirement, as-
6 sessment, or regulation promulgated under this title, may
7 be construed to preempt, displace, or supplant any Federal
8 or State common law rights or remedies, or any State stat-
9 ute creating a remedy for civil relief, including any cause
10 of action for personal injury, wrongful death, property
11 damage, or other financial, physical, reputational, or psy-
12 chological injury based in negligence, strict liability, prod-
13 ucts liability, failure to warn, an objectively offensive in-
14 trusion into the private affairs or concerns of an indi-
15 vidual, or any other legal theory of liability under any Fed-
16 eral or State common law, or any State statutory law, ex-
17 cept that the fact of a violation of this title or a regulation
18 promulgated under this title may not be pleaded as an
19 element of any violation of such law.

20 (d) NONAPPLICATION OF CERTAIN PROVISIONS OF
21 COMMUNICATIONS ACT OF 1934 AND TELECOMMUNI-
22 CATIONS ACT OF 1996 RELATED TO FCC PRIVACY AND
23 DATA SECURITY LAWS AND REGULATIONS.—

24 (1) IN GENERAL.—Except as provided in para-
25 graph (2), sections 201, 202, 222, 338(i), and 631

1 of the Communications Act of 1934 (47 U.S.C. 201;
2 202; 222; 338(i); 551) and section 706 of the Tele-
3 communications Act of 1996 (47 U.S.C. 1302), and
4 any regulation or order issued by the Federal Com-
5 munications Commission under any such section, do
6 not apply to any covered entity or service provider
7 with respect to the collection, processing, retention,
8 transfer, or security of covered data (or the equiva-
9 lent of such data), to the extent that such sections
10 or any regulation or order issued under such sec-
11 tions would otherwise cover the collection, proc-
12 essing, retention, transfer, or security of covered
13 data (or the equivalent of such data) in order to pro-
14 tect consumer privacy or the security of such data,
15 and a covered entity or service provider shall instead
16 be covered by the requirements of this title with re-
17 spect to the collection, processing, retention, trans-
18 fer, and security of covered data.

19 (2) EXCEPTIONS.—Paragraph (1) does not su-
20 persede any authority of the Federal Communica-
21 tions Commission with respect to the following:

22 (A) Emergency services (as defined in sec-
23 tion 7 of the Wireless Communications and
24 Public Safety Act of 1999 (47 U.S.C. 615b)).

1 (B) Proceedings to implement section 227
2 of the Communications Act of 1934 (47 U.S.C.
3 227) or the Pallone-Thune Telephone Robocall
4 Abuse Criminal Enforcement and Deterrence
5 Act (Public Law 116–105; 133 Stat. 3274), or
6 any other authority used by the Federal Com-
7 munications Commission to prevent or reduce
8 unwanted telephone calls or text messages.

9 (C) An enforcement action alleging or find-
10 ing a violation of a section of the Communica-
11 tions Act of 1934 specified in paragraph (1), if
12 such action was adopted by the Federal Com-
13 munications Commission prior to the date of
14 the enactment of this Act.

15 (D) Subsection (a) of section 222 of the
16 Communications Act of 1934 (47 U.S.C. 222),
17 to the extent such subsection imposes a duty on
18 every telecommunications carrier to protect the
19 confidentiality of proprietary information of,
20 and relating to, other telecommunications car-
21 riers and equipment manufacturers.

22 (E) Subsections (b), (d), and (g) of section
23 222 of the Communications Act of 1934 (47
24 U.S.C. 222).

1 (F) Any obligation of an international
2 treaty related to the exchange of traffic imple-
3 mented and enforced by the Federal Commu-
4 nications Commission.

5 **SEC. 119. CHILDREN'S ONLINE PRIVACY PROTECTION ACT**
6 **OF 1998.**

7 Nothing in this title may be construed to relieve or
8 change any obligation that a covered entity or other per-
9 son may have under the Children's Online Privacy Protec-
10 tion Act of 1998 (15 U.S.C. 6501 et seq.).

11 **SEC. 120. DATA PROTECTIONS FOR COVERED MINORS.**

12 (a) PROHIBITION ON TARGETED AND FIRST-PARTY
13 ADVERTISING TO COVERED MINORS.—A covered entity or
14 service provider acting on behalf of a covered entity may
15 not engage in targeted advertising or first-party adver-
16 tising to an individual if the covered entity has knowledge
17 that the individual is a covered minor, except that a cov-
18 ered entity or service provider may present or display to
19 a covered minor age-appropriate advertisements intended
20 for an audience of covered minors, if the covered entity
21 or service provider does not use any covered data in rela-
22 tion to such advertisements, other than data relating to
23 the status of the individual as a covered minor.

24 (b) DATA TRANSFER REQUIREMENTS RELATED TO
25 COVERED MINORS.—

1 (1) IN GENERAL.—Except as provided in para-
2 graph (2), and notwithstanding section 102(b), a
3 covered entity or a service provider acting on behalf
4 of a covered entity may not transfer or direct a serv-
5 ice provider to transfer the covered data of an indi-
6 vidual to a third party if the covered entity—

7 (A) has knowledge that the individual is a
8 covered minor; and

9 (B) has not obtained affirmative express
10 consent, unless the transfer is necessary, pro-
11 portionate, and limited to a purpose expressly
12 permitted by paragraph (2), (3), (4), (8), (9),
13 (11), (12), or (13) of section 102(d).

14 (2) EXCEPTION.—A covered entity or service
15 provider may collect, process, retain, or transfer cov-
16 ered data of an individual that the covered entity or
17 service provider knows is a covered minor in order
18 to submit information relating to child victimization
19 to law enforcement or to the nonprofit, national re-
20 source center and clearinghouse congressionally des-
21 ignated to provide assistance to victims, families,
22 child-serving professionals, and the general public on
23 missing and exploited children issues.

24 (c) RULEMAKING.—The Commission may conduct a
25 rulemaking pursuant to section 553 of title 5, United

1 States Code, to establish processes for parents and teens
2 to exercise the rights provided in this title with respect
3 to covered entities and data brokers. Any such rulemaking
4 shall take into account—

5 (1) the specific needs of parents, children, and
6 teens;

7 (2) how best to harmonize the processes pro-
8 vided for under this title with the processes and
9 guidance provided for under the Children’s Online
10 Privacy Protection Act of 1998 (15 U.S.C. 6501 et
11 seq.), as amended by title II of this Act, and any
12 regulations promulgated by the Commission there-
13 under; and

14 (3) options for reducing undue burdens on par-
15 ents, children, teens, covered entities, and data bro-
16 kers.

17 **SEC. 121. TERMINATION OF FTC RULEMAKING ON COM-**
18 **MERCIAL SURVEILLANCE AND DATA SECU-**
19 **RITY.**

20 Beginning on the date of the enactment of this Act,
21 the rulemaking proposed in the advance notice of proposed
22 rulemaking titled “Trade Regulation Rule on Commercial
23 Surveillance and Data Security” and published on August
24 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 a website, online service, on-
3 line application, or mobile application (as
4 defined in paragraph (8)(C)) of the oper-
5 ator, excluding any activity relating to tar-
6 geted advertising or first-party advertising
7 (as such terms are defined in section 101
8 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 a unique device identifier, but ex-
24 cluding an identifier that is used by an op-
25 erator solely for providing support for the

1 internal operations of a website, online
2 service, online application, or mobile appli-
3 cation;

4 “(viii) a photograph, video, or audio
5 file, if such file contains the image or voice
6 of a specific child;

7 “(ix) geolocation information;

8 “(x) information generated from the
9 measurement or technological processing of
10 the biological, physical, or physiological
11 characteristics of an individual that is used
12 to 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 the voice of a child, if the operator—

6 “(i) does not request information via
7 voice that would otherwise be considered
8 personal information under this paragraph;

9 “(ii) provides, in the privacy policy of
10 the operator, clear notice of the collection
11 and use of the audio file by the operator
12 and the deletion policy of the operator;

13 “(iii) uses the voice within the audio
14 file solely as a replacement for written
15 words, to perform a task, or to 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, online service, on-
18 line application, or mobile application, or
19 for any other purpose.”;

20 (4) by amending paragraph (9) to read as fol-
21 lows:

22 “(9) VERIFIABLE CONSENT.—The term
23 ‘verifiable consent’ means any reasonable effort (tak-
24 ing into consideration available technology), includ-
25 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) EDUCATIONAL AGENCY OR INSTITU-
17 TION.—The term ‘educational agency or institution’
18 means a State educational agency or local edu-
19 cational agency as defined under Federal law, as
20 well as an institutional day or residential school, in-
21 cluding a public school, charter school, or private
22 school, that provides elementary or secondary edu-
23 cation, as determined under State law.

24 “(15) MOBILE APPLICATION.—The term ‘mo-
25 bile application’ has the meaning given such term in

1 section 101 of the American Privacy Rights Act of
2 2024.

3 “(16) ONLINE APPLICATION.—The term ‘online
4 application’ has the meaning given such term in sec-
5 tion 101 of the American Privacy Rights Act of
6 2024.

7 “(17) PRECISE GEOLOCATION INFORMATION.—
8 The term ‘precise geolocation information’ has the
9 meaning given such term in section 101 of the
10 American Privacy Rights Act of 2024.”.

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, DISCLO-**
17 **SURE, AND DELETION OF PERSONAL INFORMA-**
18 **TION OF CHILDREN.**”;

19 (2) by amending subsection (a) to read as fol-
20 lows:

21 “(a) ACTS PROHIBITED.—It is unlawful for an oper-
22 ator of a website, online service, online application, or mo-
23 bile application directed to children or for any operator
24 of a website, online service, online application, or mobile
25 application with actual knowledge or knowledge fairly im-

1 plied on the basis of objective circumstances that a user
2 is a child—

3 “(1) to collect personal information from a child
4 in a manner that violates the American Privacy
5 Rights Act of 2024 or the regulations prescribed
6 under subsection (b); or

7 “(2) to store or transfer the personal informa-
8 tion of a child outside of the United States, unless—

9 “(A) the operator provides direct notice to
10 the parent of the child that the personal infor-
11 mation of the child is being stored or trans-
12 ferred outside of the United States; and

13 “(B) with respect to transfer, the operator
14 meets the requirements of section 102(b) of the
15 American Privacy Rights Act of 2024.”;

16 (3) in subsection (b)—

17 (A) in paragraph (1)—

18 (i) in subparagraph (A)—

19 (I) in the matter preceding clause
20 (i), by striking “operator of any
21 website” and all that follows through
22 “from a child” and inserting “oper-
23 ator of a website, online service, on-
24 line application, or mobile application
25 directed to children or that has actual

1 knowledge or knowledge fairly implied
2 on the basis of objective circumstances
3 that a user is a child”;

4 (II) in clause (i)—

5 (aa) by striking “notice on
6 the website” and inserting “clear
7 and conspicuous notice on the
8 website, service, or application”;
9 and

10 (bb) by striking “; and” and
11 inserting a semicolon;

12 (III) in clause (ii)—

13 (aa) by striking “verifiable
14 parental consent” and inserting
15 “verifiable consent”; and

16 (bb) by striking the semi-
17 colon at the end and inserting “;
18 and”; and

19 (IV) by inserting after clause (ii)
20 the following new clause:

21 “(iii) to obtain verifiable consent from
22 a parent of a child before using or dis-
23 closing personal information of the child
24 for any purpose that is a material change
25 from the original purposes and disclosure

1 practices specified to the parent of the
2 child under clause (i);”;

3 (ii) by striking subparagraph (B);

4 (iii) in subparagraph (C)—

5 (I) by striking “reasonably”; and

6 (II) by inserting “, proportionate,
7 and limited” after “necessary”;

8 (iv) in subparagraph (D), by striking
9 “website or online service” and inserting
10 “website, online service, online application,
11 or mobile application”; and

12 (v) by redesignating subparagraphs
13 (C) and (D) as subparagraphs (B) and
14 (C), respectively;

15 (B) in paragraph (2)—

16 (i) in the matter preceding subpara-
17 graph (A)—

18 (I) by striking “verifiable paren-
19 tal consent” and inserting “verifiable
20 consent”; and

21 (II) by striking “paragraph
22 (1)(A)(ii)” and inserting “clause (ii)
23 or (iii) of paragraph (1)(A)”;

- 1 (ii) in subparagraph (A), by inserting
2 “or to contact another child” after “to re-
3 contact the child”;
- 4 (iii) in subparagraph (B)—
5 (I) by striking “or child”; and
6 (II) by striking “parental con-
7 sent” each place the term appears and
8 inserting “verifiable consent”;
- 9 (iv) in subparagraph (D), in the mat-
10 ter preceding clause (i)—
11 (I) by striking “reasonably”; and
12 (II) by inserting “, proportionate,
13 and limited” after “necessary”; and
14 (v) in subparagraph (E)—
15 (I) in the matter preceding clause
16 (i), by striking “website or online
17 service” and inserting “website, online
18 service, online application, or mobile
19 application”; and
20 (II) in clause (i), by striking
21 “website” and inserting “website,
22 service, or application”;
- 23 (C) by redesignating paragraph (3) as
24 paragraph (4) and inserting after paragraph
25 (2) the following new paragraph:

1 “(3) APPLICATION TO OPERATORS ACTING
2 UNDER AGREEMENTS WITH EDUCATIONAL AGENCIES
3 OR INSTITUTIONS.—The regulations may provide
4 that verifiable consent under clause (ii) or (iii) of
5 paragraph (1)(A) is not required for an operator
6 that is acting under a written agreement with an
7 educational agency or institution that, at a min-
8 imum, requires—

9 “(A) the operator to—

10 “(i) limit its collection, use, and dis-
11 closure of the personal information from a
12 child to solely educational purposes and for
13 no other commercial purposes;

14 “(ii) provide the educational agency or
15 institution with a notice of the specific
16 types of personal information the operator
17 will collect from the child, the method by
18 which the operator will obtain the personal
19 information, and the purposes for which
20 the operator will collect, use, disclose, and
21 retain the personal information;

22 “(iii) provide the educational agency
23 or institution with a link to the online no-
24 tice of information practices of the oper-

1 ator as required under paragraph
2 (1)(A)(i); and

3 “(iv) provide the educational agency
4 or institution, upon request, with a means
5 to review the personal information collected
6 from a child, to prevent further use or
7 maintenance or future collection of per-
8 sonal information from a child, and to de-
9 lete personal information collected from a
10 child or content or information submitted
11 by a child to the website, online service,
12 online application, or mobile application of
13 the operator;

14 “(B) a representative of the educational
15 agency or institution to—

16 “(i) acknowledge and agree that the
17 representative has authority to authorize
18 the collection, use, and disclosure of per-
19 sonal information from children on behalf
20 of the educational agency or institution;
21 and

22 “(ii) provide the name of the rep-
23 resentative and the title of the representa-
24 tive at the educational agency or institu-
25 tion; and

1 “(C) the educational agency or institution
2 to—

3 “(i) provide on the website of the edu-
4 cational agency or institution a notice that
5 identifies the operator with which the edu-
6 cational agency or institution has entered
7 into a written agreement under this para-
8 graph and a link to the online notice of in-
9 formation practices of the operator as re-
10 quired under paragraph (1)(A)(i);

11 “(ii) provide the notice of the operator
12 regarding the information practices of the
13 operator, as required under subparagraph
14 (A)(ii), upon 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 collected
18 from the child of the parent and provide
19 the parent a means to review the personal
20 information.”;

21 (D) by amending paragraph (4), as so re-
22 designated, to read as follows:

23 “(4) TERMINATION OF SERVICE.—The regula-
24 tions shall permit the operator of a website, online
25 service, online application, or mobile application to

1 terminate service provided to a child whose parent
2 has requested to delete covered data of the child
3 pursuant to section 105 of the American Privacy
4 Rights Act of 2024.”; and

5 (E) by adding at the end the following new
6 paragraphs:

7 “(5) CONTINUATION OF SERVICE.—The regula-
8 tions shall prohibit an operator from discontinuing
9 service provided to a child on the basis of a request
10 by the parent of the child to delete personal informa-
11 tion collected from the child, to the extent that the
12 operator is capable of providing such service without
13 such information.

14 “(6) COMMON VERIFIABLE CONSENT MECHA-
15 NISM.—

16 “(A) IN GENERAL.—

17 “(i) FEASIBILITY OF MECHANISM.—
18 The Commission shall conduct an assess-
19 ment, with notice and public comment, of
20 the feasibility of allowing operators the op-
21 tion to use a common verifiable consent
22 mechanism that fully meets the require-
23 ments of this title.

24 “(ii) REQUIREMENTS.—The feasibility
25 assessment described in clause (i) shall

1 consider whether a single operator could
2 use a common verifiable consent mecha-
3 nism to obtain verifiable consent, as re-
4 quired under this title, from a parent of a
5 child on behalf of multiple, listed operators
6 that provide a joint or related service.

7 “(B) REPORT.—Not later than 1 year
8 after the date of the enactment of this para-
9 graph, the Commission shall submit to the
10 Committee on Commerce, Science, and Trans-
11 portation of the Senate and the Committee on
12 Energy and Commerce of the House of Rep-
13 resentatives a report with the findings of the
14 assessment required by subparagraph (A).

15 “(C) REGULATIONS.—If the Commission
16 finds, in the assessment required by subpara-
17 graph (A), that the use of a common verifiable
18 consent mechanism is feasible and would meet
19 the requirements of this title, the Commission
20 shall issue regulations, pursuant to section 553
21 of title 5, United States Code, to permit the use
22 of a common verifiable consent mechanism in
23 accordance with the findings outlined in the re-
24 port submitted under subparagraph (B).”;

1 (4) in subsection (c), by striking “a regulation
2 prescribed under subsection (a)” and inserting
3 “paragraph (2) of subsection (a), or of a regulation
4 prescribed under subsection (b),”; and

5 (5) by striking subsection (d) and inserting the
6 following:

7 “(d) RELATIONSHIP TO STATE LAW.—The provisions
8 of this title shall preempt any State law, rule, or regula-
9 tion only to the extent that such State law, rule, or regula-
10 tion conflicts with a provision of this title. Nothing in this
11 title may be construed to prohibit any State from enacting
12 a law, rule, or regulation that provides greater protection
13 to children than the provisions of this title.”.

14 (c) SAFE HARBORS.—Section 1304 of the Children’s
15 Online Privacy Protection Act of 1998 (15 U.S.C. 6503)
16 is amended by adding at the end the following:

17 “(d) PUBLICATION.—

18 “(1) IN GENERAL.—Subject to the restrictions
19 described in paragraph (2), the Commission shall
20 publish on the website of the Commission any report
21 or documentation required by regulation to be sub-
22 mitted to the Commission to carry out this section.

23 “(2) RESTRICTIONS ON PUBLICATION.—The re-
24 strictions described in sections 6(f) and 21 of the
25 Federal Trade Commission Act (15 U.S.C. 46(f);

1 57b–2) applicable to the disclosure of information
2 obtained by the Commission shall apply in the same
3 manner to the disclosure under this subsection of in-
4 formation obtained by the Commission from a report
5 or documentation described in paragraph (1).”.

6 (d) ACTIONS BY STATES.—Section 1305 of the Chil-
7 dren’s Online Privacy Protection Act of 1998 (15 U.S.C.
8 6504) is amended—

9 (1) in subsection (a)(1)—

10 (A) in the matter preceding subparagraph
11 (A), by inserting “section 1303(a) or” before
12 “any regulation”; and

13 (B) in subparagraph (B), by striking “the
14 regulation” and inserting “such section or regu-
15 lation”; and

16 (2) in subsection (d)—

17 (A) by inserting “section 1303(a) or” be-
18 fore “any regulation”; and

19 (B) by striking “that regulation” and in-
20 serting “such section or regulation”.

21 (e) ADMINISTRATION AND APPLICABILITY OF ACT.—
22 Section 1306 of the Children’s Online Privacy Protection
23 Act of 1998 (15 U.S.C. 6505) is amended—

24 (1) in subsection (d)—

1 (A) by inserting “section 1303(a) or” be-
2 fore “a rule”; and

3 (B) by striking “such rule” and inserting
4 “section 1303(a) or a rule of the Commission
5 under section 1303”; and

6 (2) by adding at the end the following new sub-
7 sections:

8 “(f) DETERMINATION OF WHETHER AN OPERATOR
9 HAS KNOWLEDGE FAIRLY IMPLIED ON THE BASIS OF
10 OBJECTIVE CIRCUMSTANCES.—

11 “(1) RULE OF CONSTRUCTION.—For purposes
12 of enforcing this title or a regulation promulgated
13 under this title, in making a determination as to
14 whether an operator has knowledge fairly implied on
15 the basis of objective circumstances that a specific
16 user is a child, the Commission or a State attorney
17 general shall rely on competent and reliable evi-
18 dence, taking into account the totality of the cir-
19 cumstances, including whether a reasonable and pru-
20 dent person under the circumstances would have
21 known that the user is a child. Nothing in this title,
22 including a determination described in the preceding
23 sentence, may be construed to require an operator
24 to—

1 “(A) affirmatively collect any personal in-
2 formation with respect to the age of a child that
3 an operator is not already collecting in the nor-
4 mal course of business; or

5 “(B) implement an age gating or age
6 verification functionality.

7 “(2) COMMISSION GUIDANCE.—

8 “(A) IN GENERAL.—Not later than 180
9 days after the date of the enactment of this
10 subsection, the Commission shall issue guidance
11 to provide information, including best practices
12 and examples, for operators to understand the
13 process of the Commission for determining
14 whether an operator has knowledge fairly im-
15 plied on the basis of objective circumstances
16 that a user is a child.

17 “(B) LIMITATION.—No guidance issued by
18 the Commission under subparagraph (A) con-
19 fers any rights on any person, State, or locality,
20 or operates to bind the Commission or any per-
21 son, State, or locality to the approach rec-
22 ommended in such guidance. In any enforce-
23 ment action brought pursuant to this title, the
24 Commission or State attorney general, as appli-
25 cable, shall allege a specific violation of a provi-

1 sion of this title, and the Commission or State
2 attorney general, as applicable, may not base an
3 enforcement action on, or execute a consent
4 order based on, practices that are alleged to be
5 inconsistent with any such guidance, unless the
6 practices allegedly violate this title.

7 “(g) **ADDITIONAL REQUIREMENT.**—Any regulations
8 issued under this title shall include a description and anal-
9 ysis of the impact of proposed and final rules on small
10 entities per chapter 6 of title 5, United States Code.”.

11 **SEC. 203. STUDY AND REPORTS ON MOBILE AND ONLINE**
12 **APPLICATION OVERSIGHT AND ENFORCE-**
13 **MENT.**

14 (a) **OVERSIGHT REPORT.**—Not later than 3 years
15 after the date of the enactment of this Act, the Federal
16 Trade Commission shall submit to the Committee on Com-
17 merce, Science, and Transportation of the Senate and the
18 Committee on Energy and Commerce of the House of
19 Representatives a report on the processes of platforms
20 that offer mobile and online applications for ensuring that,
21 for those applications that are websites, online services,
22 online applications, or mobile applications directed to chil-
23 dren, the applications operate in accordance with—

1 (1) this title, the amendments made by this
2 title, and any rules promulgated under this title or
3 the amendments made by this title; and

4 (2) rules promulgated by the Commission under
5 section 18 of the Federal Trade Commission Act (15
6 U.S.C. 57a) relating to unfair or deceptive acts or
7 practices in marketing.

8 (b) ENFORCEMENT REPORT.—Not later than 1 year
9 after the date of the enactment of this Act, and annually
10 thereafter, the Federal Trade Commission shall submit to
11 the Committee on Commerce, Science, and Transportation
12 of the Senate and the Committee on Energy and Com-
13 merce of the House of Representatives a report that ad-
14 dresses, at a minimum—

15 (1) the number of actions brought by the Com-
16 mission during the reporting year to enforce the
17 Children’s Online Privacy Protection Act of 1998
18 (15 U.S.C. 6501 et seq.) and the outcome of each
19 such action;

20 (2) the total number of investigations or inquir-
21 ies into potential violations of such Act commenced
22 during the reporting year;

23 (3) the total number of open investigations or
24 inquiries into potential violations of such Act as of
25 the time the report is submitted;

1 (4) the number and nature of complaints re-
2 ceived by the Commission relating to an allegation
3 of a violation of such Act during the reporting year;
4 and

5 (5) policy or legislative recommendations to
6 strengthen online protections for children.

7 (c) REPORT BY THE INSPECTOR GENERAL.—

8 (1) IN GENERAL.—Not later than 2 years after
9 the date of the enactment of this Act, the Inspector
10 General of the Federal Trade Commission shall sub-
11 mit to the Federal Trade Commission and to the
12 Committee on Commerce, Science, and Transpor-
13 tation of the Senate and the Committee on Energy
14 and Commerce of the House of Representatives a re-
15 port regarding the safe harbor provisions in section
16 1304 of the Children’s Online Privacy Protection
17 Act of 1998 (15 U.S.C. 6503), which shall include—

18 (A) an analysis of whether the safe harbor
19 provisions are—

20 (i) operating fairly and effectively;

21 and

22 (ii) effectively protecting the interests
23 of children; and

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

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

8 **SEC. 204. SEVERABILITY.**

9 If any provision of this title or the amendments made
10 by this title, or the application thereof to any person or
11 circumstance, is held invalid, the remainder of this title
12 and the amendments made by this title, and the applica-
13 tion of such provision to other persons not similarly situ-
14 ated or to other circumstances, may not be affected by
15 the invalidation.

○