

**AMENDMENT IN THE NATURE OF A SUBSTITUTE  
TO H.R. 7890**

**OFFERED BY \_\_\_\_\_**

Strike all after the enacting clause and insert the following:

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

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

4 (b) TABLE OF CONTENTS.—The table of contents for  
5 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. Relation to other Federal laws.
- Sec. 118. Children’s Online Privacy Protection Act of 1998.
- Sec. 119. Data protections for covered minors.
- Sec. 120. Termination of FTC rulemaking on commercial surveillance and data security.
- Sec. 121. Severability.
- Sec. 122. Innovation rulemakings.
- Sec. 123. 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—

9                               (i) clearly communicates the author-  
10                              ization of the individual for an act or prac-  
11                              tice; and

12                             (ii) is provided in response to a spe-  
13                             cific request from a covered entity, or a  
14                             service provider on behalf of a covered en-  
15                             tity, that meets the requirements of sub-  
16                             paragraph (B).

17               (B) **REQUEST REQUIREMENTS.**—The re-  
18               quirements of this subparagraph with respect to  
19               a request are the following:

20                             (i) The request is provided to the indi-  
21                             vidual in a clear and conspicuous stand-  
22                             alone disclosure.

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

4 (I) clearly distinguishes between  
5 an act or practice that is necessary,  
6 proportionate, and limited to fulfill a  
7 request of the individual and an act or  
8 practice that is for another purpose;

9 (II) clearly states the specific  
10 categories of covered data that the  
11 covered entity shall collect, process,  
12 retain, or transfer under each such  
13 act or practice; and

14 (III) is written in easy-to-under-  
15 stand language and includes a promi-  
16 nent heading that would enable a rea-  
17 sonable individual to identify and un-  
18 derstand each such act or practice.

19 (iii) The request clearly explains the  
20 applicable rights of the individual related  
21 to consent.

22 (iv) The request is made in a manner  
23 reasonably accessible to and usable by indi-  
24 viduals living with disabilities.

1           (v) The request is made available to  
2           the individual in the language in which the  
3           covered entity provides a product or service  
4           for which authorization is sought.

5           (vi) The option to refuse consent is at  
6           least as prominent as the option to provide  
7           consent, and the option to refuse consent  
8           takes no more than 1 additional step as  
9           compared to the number of steps necessary  
10          to provide consent.

11          (vii) With respect to affirmative ex-  
12          press consent sought for the collection,  
13          processing, retention, or transfer of bio-  
14          metric information or genetic information,  
15          the request includes the length of time the  
16          covered entity or service provider intends  
17          to retain the biometric information or ge-  
18          netic information or, if it is not possible to  
19          identify the length of time, the criteria  
20          used to determine the length of time the  
21          covered entity or service provider intends  
22          to retain the biometric information or ge-  
23          netic information.

24          (C) EXPRESS CONSENT REQUIRED.—Af-  
25          firmative express consent to an act or practice

1           may not be inferred from the inaction of an in-  
2           dividual or the continued use by an individual  
3           of a service or product provided by an entity.

4           (D) WITHDRAWAL OF AFFIRMATIVE EX-  
5           PRESS CONSENT.—

6           (i) IN GENERAL.—A covered entity  
7           shall provide an individual with a means to  
8           withdraw affirmative express consent pre-  
9           viously provided by the individual.

10          (ii) REQUIREMENTS.—The means to  
11          withdraw affirmative express consent de-  
12          scribed in clause (i) shall be—

13                   (I) clear and conspicuous; and

14                   (II) as easy for a reasonable indi-  
15                   vidual to use as the mechanism by  
16                   which the individual provided affirma-  
17                   tive express consent.

18          (E) CHILDREN AND TEENS.—If a covered  
19          entity has knowledge that—

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

23                   (ii) an individual is a teen, a parent or  
24                   the teen may provide affirmative express  
25                   consent on behalf of the teen.

1 (2) BIOMETRIC INFORMATION.—

2 (A) IN GENERAL.—The term “biometric  
3 information” means any covered data that al-  
4 lows or confirms the unique identification or  
5 verification of an individual and is generated  
6 from the measurement or processing of unique  
7 biological, physical, or physiological characteris-  
8 tics, including—

9 (i) fingerprints;

10 (ii) voice prints;

11 (iii) iris or retina imagery scans;

12 (iv) facial or hand mapping, geometry,  
13 or templates; and

14 (v) gait.

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

17 (i) a digital or physical photograph;

18 (ii) an audio or video recording; or

19 (iii) data derived from a digital or  
20 physical photograph or an audio or video  
21 recording that cannot be used to identify  
22 or authenticate a specific individual.

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

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

5           (5) COARSE GEOLOCATION INFORMATION.—The  
6           term “coarse geolocation information” means infor-  
7           mation that reveals the present physical location of  
8           an individual or device identified by a unique per-  
9           sistent identifier at the ZIP Code attribution level  
10          (except, if a geographic area attributed to a ZIP  
11          Code is equal to or less than the area of a circle  
12          with a radius of 1,850 feet or less, at a level greater  
13          than a geographic area equal to the area of a circle  
14          with a radius of 1,850 feet).

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

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

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

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

4           (10) CONTEXTUAL ADVERTISING.—The term  
5           “contextual advertising” means displaying or pre-  
6           senting an advertisement that—

7                   (A) does not vary based on the identity of  
8                   the individual recipient; and

9                   (B) is based solely on—

10                          (i) the content of a webpage or online  
11                          service;

12                          (ii) a specific request of the individual  
13                          for information or feedback; or

14                          (iii) coarse geolocation information.

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

17                   (A) ownership of, or the power to vote,  
18                   more than 50 percent of the outstanding shares  
19                   of any class of voting security of the entity;

20                   (B) control over the election of a majority  
21                   of the directors of the entity (or of individuals  
22                   exercising similar functions); or

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

25           (12) COVERED DATA.—



1 (A) IN GENERAL.—The term “covered  
2 data” means information that identifies or is  
3 linked or reasonably linkable, alone or in com-  
4 bination with other information, to an indi-  
5 vidual or a device that identifies or is linked or  
6 reasonably linkable to 1 or more individuals.

7 (B) EXCLUSIONS.—The term “covered  
8 data” does not include—

- 9 (i) de-identified data;  
10 (ii) employee information;  
11 (iii) publicly available information;  
12 (iv) inferences made exclusively from  
13 multiple independent sources of publicly  
14 available information, if such inferences—

15 (I) do not reveal information  
16 about an individual that meets the  
17 definition of the term “sensitive cov-  
18 ered data” with respect to the indi-  
19 vidual; and

20 (II) are not combined with cov-  
21 ered data;

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

24 (I) the collection is—

1 (aa) open to the public or  
2 routinely made available to re-  
3 searchers who are not affiliated  
4 with the library, archive, or mu-  
5 seum; and

6 (bb) composed of lawfully  
7 acquired materials with respect  
8 to which all licensing conditions  
9 are met; and

10 (II) the library, archive, or mu-  
11 seum has—

12 (aa) a public service mission;  
13 and

14 (bb) trained staff or volun-  
15 teers to provide professional serv-  
16 ices normally associated with li-  
17 braries, archives, or museums; or

18 (vi) on-device data.

19 (13) COVERED ENTITY.—

20 (A) IN GENERAL.—The term “covered en-  
21 tity” means any entity that, alone or jointly  
22 with others, determines the purposes and means  
23 of collecting, processing, retaining, or transfer-  
24 ring covered data and—

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

3 (ii) is a common carrier subject to  
4 title II of the Communications Act of 1934  
5 (47 U.S.C. 201 et seq.); or

6 (iii) is an organization not organized  
7 to carry on business for its own profit or  
8 that of its members.

9 (B) INCLUSION.—The term “covered enti-  
10 ty” includes any entity that controls, is con-  
11 trolled by, or is under common control with an-  
12 other covered entity.

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

15 (i) a Federal, State, Tribal, or local  
16 government entity, such as a body, author-  
17 ity, board, bureau, commission, district,  
18 agency, or other political subdivision of the  
19 Federal Government or a State, Tribal, or  
20 local government;

21 (ii) an entity that is collecting, proc-  
22 essing, retaining, or transferring covered  
23 data on behalf of a Federal, State, Tribal,  
24 or local government entity, to the extent

1 that such entity is acting as a service pro-  
2 vider to the government entity;

3 (iii) a small business;

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

6 (v) the National Center for Missing  
7 and Exploited Children; or

8 (vi) except with respect to require-  
9 ments under section 109, a nonprofit orga-  
10 nization whose primary mission is to pre-  
11 vent, investigate, or deter fraud, to train  
12 anti-fraud professionals, or to educate the  
13 public about fraud, including insurance  
14 fraud, securities fraud, and financial fraud,  
15 to the extent the organization collects,  
16 processes, retains, or transfers covered  
17 data in furtherance of such primary mis-  
18 sion.

19 (D) NONAPPLICATION TO SERVICE PRO-  
20 VIDERS.—An entity may not be considered to  
21 be a “covered entity” for the purposes of this  
22 title, insofar as the entity is acting as a service  
23 provider.

24 (14) COVERED HIGH-IMPACT SOCIAL MEDIA  
25 COMPANY.—

1 (A) IN GENERAL.—The term “covered  
2 high-impact social media company” means a  
3 covered entity that provides any internet-acces-  
4 sible platform that—

5 (i) generates \$3,000,000,000 or more  
6 in global annual revenue, including the rev-  
7 enue generated by any affiliate of such cov-  
8 ered entity;

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

12 (iii) constitutes an online product or  
13 service that is primarily used by users to  
14 access or share user-generated content.

15 (B) TREATMENT OF CERTAIN SERVICES  
16 AND APPLICATIONS.—A service or application  
17 may not be considered to constitute an online  
18 product or service described in subparagraph  
19 (A)(iii) solely on the basis of providing any of  
20 the following:

21 (i) Email.

22 (ii) Career or professional develop-  
23 ment networking opportunities.

24 (iii) Reviews of products, services,  
25 events, or destinations.

1 (iv) A platform for use in a public or  
2 private school under the direction of the  
3 school.

4 (v) File collaboration.

5 (vi) Cloud storage.

6 (vii) Closed video or audio commu-  
7 nications services.

8 (viii) A wireless messaging service, in-  
9 cluding such a service provided through  
10 short messaging service or multimedia  
11 messaging service protocols, that is not a  
12 component of, or linked to, a platform of  
13 a covered high-impact social media com-  
14 pany, if the predominant or exclusive func-  
15 tion is direct messaging consisting of the  
16 transmission of text, photos, or videos that  
17 are sent by electronic means, and if mes-  
18 sages are transmitted from the sender to a  
19 recipient and are not posted within a plat-  
20 form of a covered high-impact social media  
21 company or publicly.

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

24 (16) DARK PATTERNS.—The term “dark pat-  
25 terns” means a user interface designed or manipu-

1       lated with the substantial effect of subverting or im-  
2       pairing user autonomy, decision-making, or choice.

3               (17) DATA BROKER.—

4               (A) IN GENERAL.—The term “data  
5       broker” means a covered entity whose principal  
6       source of revenue is derived from processing or  
7       transferring covered data that the covered enti-  
8       ty did not collect directly from the individuals  
9       linked or linkable to the covered data.

10              (B) PRINCIPAL SOURCE OF REVENUE.—  
11       For purposes of this paragraph, the term “prin-  
12       cipal source of revenue” means, for the prior  
13       12-month period—

14              (i) revenue that constitutes greater  
15       than 50 percent of all revenue of the cov-  
16       ered entity during such period; or

17              (ii) revenue obtained from processing  
18       and transferring the covered data of more  
19       than 5,000,000 individuals that the cov-  
20       ered entity did not collect directly from the  
21       individuals linked or linkable to the cov-  
22       ered data.

23              (C) NON-APPLICATION TO SERVICE PRO-  
24       VIDERS.—The term “data broker” does not in-

1           clude an entity to the extent that such entity is  
2           acting as a service provider.

3           (18) DE-IDENTIFIED DATA.—

4                   (A) IN GENERAL.—The term “de-identified  
5           data” means information that cannot reason-  
6           ably be used to infer or derive the identity of  
7           an individual, and does not identify and is not  
8           linked or reasonably linkable to an individual or  
9           a device that identifies or is linked or reason-  
10          ably linkable to an individual, regardless of  
11          whether the information is aggregated, if the  
12          relevant covered entity or service provider—

13                           (i) takes reasonable physical, adminis-  
14                           trative, and technical measures to ensure  
15                           that the information cannot, at any point,  
16                           be used to re-identify any individual or de-  
17                           vice that identifies or is linked or reason-  
18                           ably linkable to an individual;

19                           (ii) publicly commits in a clear and  
20                           conspicuous manner to—

21                                   (I) process, retain, or transfer  
22                                   the information solely in a de-identi-  
23                                   fied form without any reasonable  
24                                   means for re-identification; and



1 (II) not attempt to re-identify the  
2 information with any individual or de-  
3 vice that identifies or is linked or rea-  
4 sonably linkable to an individual, ex-  
5 cept as necessary, limited, and propor-  
6 tionate to test the effectiveness of the  
7 measures described in clause (i); and  
8 (iii) contractually obligates any entity  
9 that receives the information from the cov-  
10 ered entity or service provider to—

11 (I) comply with clauses (i) and  
12 (ii) with respect to the information;  
13 and

14 (II) require that such contractual  
15 obligations be included contractually  
16 in all subsequent instances in which  
17 the information may be received.

18 (B) HEALTH INFORMATION.—The term  
19 “de-identified data” includes health information  
20 (as defined in section 1171 of the Social Secu-  
21 rity Act (42 U.S.C. 1320d)) that has been de-  
22 identified in accordance with section 164.514(b)  
23 of title 45, Code of Federal Regulations, except  
24 that if such information is subsequently pro-  
25 vided to an entity that is not an entity subject

1 to parts 160 and 164 of such title 45, such en-  
2 tity shall comply with clauses (ii) and (iii) of  
3 subparagraph (A) for the information to be con-  
4 sidered de-identified under this title.

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

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

15 (21) DIRECT MAIL TARGETED ADVERTISING.—  
16 The term “direct mail targeted advertising” means  
17 advertising or marketing using third-party data  
18 through a direct communication with an individual  
19 via direct mail.

20 (22) DISABILITY.—The term “disability” has  
21 the meaning given such term in section 3 of the  
22 Americans with Disabilities Act of 1990 (42 U.S.C.  
23 12102).

24 (23) EMAIL TARGETED ADVERTISING.—The  
25 term “email targeted advertising” means advertising

1 or marketing using third-party data through a direct  
2 communication with an individual via email.

3 (24) EMPLOYEE.—The term “employee” means  
4 an individual who is an employee, director, officer,  
5 staff member, paid intern, individual working as an  
6 independent contractor (who is not a service pro-  
7 vider), volunteer, or unpaid intern of an employer,  
8 regardless of whether such individual is paid, un-  
9 paid, or engaged on a temporary basis.

10 (25) EMPLOYEE INFORMATION.—The term  
11 “employee information” means information, includ-  
12 ing biometric information or genetic information—

13 (A) about an individual related to the  
14 course of employment or application for employ-  
15 ment of the individual (including on a contract  
16 or temporary basis), if such information is col-  
17 lected, retained, processed, or transferred by  
18 the employer or the service provider of the em-  
19 ployer solely for purposes necessary for the em-  
20 ployment or application of the individual;

21 (B) that is emergency contact information  
22 for an individual who is an employee or job ap-  
23 plicant of an employer, if such information is  
24 collected, retained, processed, or transferred by  
25 the employer or the service provider of the em-

1           employer solely for the purpose of having an emer-  
2           gency contact for such individual on file; or

3           (C) about an individual who is an employee  
4           or former employee of an employer, or a rel-  
5           ative, dependent, or beneficiary of the employee  
6           or former employee, and collected, retained,  
7           processed, or transferred for the purpose of ad-  
8           ministering benefits, including enrollment and  
9           disenrollment for benefits, to which the em-  
10          ployee, former employee, relative, dependent, or  
11          beneficiary is entitled on the basis of the em-  
12          ployment of the employee or former employee  
13          with the employer, if such information is col-  
14          lected, retained, processed, or transferred by  
15          the employer or the service provider of the em-  
16          ployer solely for the purpose of administering  
17          such benefits.

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

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

24          (28) FEDERATED NONPROFIT ORGANIZA-  
25          TION.—The term “federated nonprofit organization”

1 means a network or system of 2 or more entities, de-  
2 scribed in section 501(c)(3) of the Internal Revenue  
3 Code of 1986 and exempt from taxation under sec-  
4 tion 501(a) of such Code, that share common brand-  
5 ing.

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

7 (A) means a consumer-facing covered enti-  
8 ty with which a consumer intends and expects  
9 to interact; and

10 (B) includes any entities with which the  
11 covered entity shares common branding.

12 (30) FIRST-PARTY ADVERTISING.—

13 (A) IN GENERAL.—The term “first-party  
14 advertising” means advertising or marketing by  
15 a first party using the first-party data of the  
16 first party and not other forms of covered data  
17 and carried out—

18 (i) through direct communications  
19 with an individual, such as direct mail,  
20 email (subject to the CAN-SPAM Act of  
21 2003 (15 U.S.C. 7701 et seq.) and the  
22 regulations promulgated under such Act),  
23 or text message communications (subject  
24 to section 227 of the Communications Act

1 of 1934 (47 U.S.C. 227) and the regula-  
2 tions promulgated under such section); or

3 (ii) entirely—

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

6 (II) in the case of a first party  
7 that is not a covered high-impact so-  
8 cial media company, on a website, on-  
9 line service, online application, or mo-  
10 bile application operated by the first  
11 party, through display or presentation  
12 of an online advertisement that pro-  
13 motes a product or service (whether  
14 offered by the first party or not of-  
15 fered by the first party) to an indi-  
16 vidual or device identified by a unique  
17 persistent identifier, or group of indi-  
18 viduals or devices identified by unique  
19 persistent identifiers; or

20 (III) in the case of a first party  
21 that is a covered high-impact social  
22 media company, on a website, online  
23 service, online application, or mobile  
24 application operated by the first  
25 party, through display or presentation

1 of an online advertisement that pro-  
2 motes a product or service offered by  
3 the first party to an individual or de-  
4 vice identified by a unique persistent  
5 identifier, or group of individuals or  
6 devices identified by unique persistent  
7 identifiers.

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

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

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

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

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

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

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

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

16          (35) KNOWLEDGE.—

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

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



1 implied on the basis of objective circumstances  
2 that an individual is a child, teen, or covered  
3 minor shall rely on competent and reliable evi-  
4 dence, taking into account the totality of the  
5 circumstances, including whether a reasonable  
6 and prudent person under the circumstances  
7 would have known that the individual is a child,  
8 teen, or covered minor. Nothing in this title, in-  
9 cluding a determination described in the pre-  
10 ceeding sentence, may be construed to require a  
11 covered entity to—

12 (i) affirmatively collect any covered  
13 data with respect to the age of a child,  
14 teen, or covered minor that the covered en-  
15 tity is not already collecting in the normal  
16 course of business; or

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

19 (C) COMMISSION GUIDANCE.—

20 (i) IN GENERAL.—Not later than 180  
21 days after the date of the enactment of  
22 this Act, the Commission shall issue guid-  
23 ance to provide information, including best  
24 practices and examples, for covered entities  
25 to use in understanding whether a covered

1           entity has knowledge fairly implied on the  
2           basis of objective circumstances that an in-  
3           dividual is a child, teen, or covered minor.

4           (ii) LIMITATION.—No guidance issued  
5           by the Commission under clause (i) confers  
6           any rights on any person, State, or local-  
7           ity, or operates to bind the Commission or  
8           any person, State, or locality to the ap-  
9           proach recommended in such guidance.  
10          Any enforcement action brought pursuant  
11          to this title by the Commission, or by the  
12          attorney general of a State, the chief con-  
13          sumer protection officer of a State, or an  
14          officer or office of a State authorized to  
15          enforce privacy or data security laws appli-  
16          cable to covered entities or service pro-  
17          viders, shall allege a specific violation of a  
18          provision of this title, and the Commission  
19          or the attorney general, chief consumer  
20          protection officer, or other authorized offi-  
21          cer or office of the State, as applicable,  
22          may not base an enforcement action on, or  
23          as applicable execute a consent order based  
24          on, practices that are alleged to be incon-

1                   sistent with any such guidance, unless the  
2                   practices allegedly violate this title.

3                   (36) LARGE DATA HOLDER.—

4                   (A) IN GENERAL.—The term “large data  
5                   holder” means a covered entity or service pro-  
6                   vider that, in the most recent calendar year,  
7                   had an annual gross revenue of not less than  
8                   \$250,000,000 and, subject to subparagraph  
9                   (B), collected, processed, retained, or trans-  
10                  ferred—

11                  (i) the covered data of—

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

14                               (II) more than 15,000,000 port-  
15                               able connected devices that identify or  
16                               are linked or reasonably linkable to 1  
17                               or more individuals; or

18                               (III) more than 35,000,000 con-  
19                               nected devices that identify or are  
20                               linked or reasonable linkable to 1 or  
21                               more individuals; or

22                  (ii) the sensitive covered data of—

23                               (I) more than 200,000 individ-  
24                               uals;

1 (II) more than 300,000 portable  
2 connected devices that identify or are  
3 linked or reasonable linkable to 1 or  
4 more individuals; or

5 (III) more than 700,000 con-  
6 nected devices that identify or are  
7 linked or reasonably linkable to 1 or  
8 more individuals.

9 (B) EXCLUSIONS.—For the purposes of  
10 subparagraph (A), a covered entity or service  
11 provider may not be considered a large data  
12 holder solely on the basis of collecting, proc-  
13 essing, retaining, or transferring to a service  
14 provider—

15 (i) personal mailing or email address-  
16 es;

17 (ii) personal telephone numbers;

18 (iii) log-in information of an indi-  
19 vidual or device to allow the individual or  
20 device to log in to an account administered  
21 by the covered entity; or

22 (iv) in the case of a covered entity  
23 that is a seller of goods or services (other  
24 than an entity that facilitates payment,  
25 such as a bank, credit card processor, mo-

1           bile payment system, or payment plat-  
2           form), credit, debit, or mobile payment in-  
3           formation necessary and used to initiate,  
4           render, bill for, finalize, complete, or other-  
5           wise facilitate payments for such goods or  
6           services.

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

11                 (i) means the gross receipts the cov-  
12                 ered entity or service provider received, in  
13                 whatever form from all sources, without  
14                 subtracting any costs or expenses; and

15                 (ii) includes contributions, gifts,  
16                 grants, dues or other assessments, income  
17                 from investments, and proceeds from the  
18                 sale of real or personal property.

19          (37) MARKET RESEARCH.—The term “market  
20          research” means the collection, processing, retention,  
21          or transfer of covered data, with affirmative express  
22          consent, that is necessary, proportionate, and limited  
23          to measure and analyze the market or market trends  
24          of products, services, advertising, or ideas, if the  
25          covered data is not—

1 (A) integrated into any product or service;

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

4 (C) used for targeted advertising or to oth-  
5 erwise market to any individual or device of an  
6 individual.

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

15 (39) MOBILE APPLICATION.—The term “mobile  
16 application”—

17 (A) means a software program that runs  
18 on the operating system of—

19 (i) a cellular telephone;

20 (ii) a tablet computer; or

21 (iii) a similar portable computing de-  
22 vice that transmits data over a wireless  
23 connection; and

24 (B) includes a service or application of-  
25 fered via a connected device.

1 (40) ON-DEVICE DATA.—

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

5 (B) LIMITATION.—Data collected, re-  
6 tained, and processed solely on the device of an  
7 individual may be considered “on-device data”  
8 only if—

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

11 (ii) the relevant covered entity clearly  
12 and conspicuously provides the device  
13 owner with controls that allow the owner  
14 to access, correct, delete, and export such  
15 data consistent with the rights provided  
16 with respect to covered data pursuant to  
17 section 105;

18 (iii) the relevant covered entity pro-  
19 vides easy-to-understand instructions on  
20 how the device owner can access such con-  
21 trols; and

22 (iv) the relevant covered entity estab-  
23 lishes, implements, and maintains reason-  
24 able data security practices, consistent  
25 with section 109, to protect—

1 (I) the confidentiality, integrity,  
2 and availability of the on-device data;  
3 and

4 (II) on device data against unau-  
5 thORIZED access.

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

16 (42) ONLINE APPLICATION.—The term “online  
17 application”—

18 (A) means an internet-connected software  
19 program; and

20 (B) includes a service or application of-  
21 fered via a connected device.

22 (43) PARENT.—The term “parent” means a  
23 legal guardian.

24 (44) PORTABLE CONNECTED DEVICE.—The  
25 term “portable connected device” means a portable



1 device that is capable of connecting to the internet  
2 over a wireless connection, including a smartphone,  
3 tablet computer, laptop computer, smartwatch, or  
4 similar portable device.

5 (45) PRECISE GEOLOCATION INFORMATION.—

6 (A) IN GENERAL.—The term “precise  
7 geolocation information” means information  
8 that reveals the past or present physical loca-  
9 tion of an individual or device with sufficient  
10 precision to identify the location of such indi-  
11 vidual or device within a geographic area that  
12 is equal to or less than the area of a circle with  
13 a radius of 1,850 feet or less.

14 (B) EXCLUSIONS.—The term “precise  
15 geolocation information” does not include infor-  
16 mation derived solely from—

- 17 (i) a digital or physical photograph;  
18 (ii) an audio or visual recording; or  
19 (iii) metadata associated with a digital  
20 or physical photograph or an audio or vis-  
21 ual recording that cannot be linked to an  
22 individual.

23 (46) PROCESS.—The term “process” means,  
24 with respect to covered data, any operation or set of  
25 operations performed on the covered data, including

1 analyzing, organizing, structuring, using, modifying,  
2 or otherwise handling the covered data.

3 (47) PUBLICLY AVAILABLE INFORMATION.—

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

9 (i) Federal, State, or local government  
10 records, if the covered entity collects, proc-  
11 esses, retains, and transfers such informa-  
12 tion in accordance with any restrictions or  
13 terms of use placed on the information by  
14 the relevant government entity;

15 (ii) widely distributed media;

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

21 (iv) a disclosure to the general public  
22 that is required to be made by Federal,  
23 State, or local law.

24 (B) CLARIFICATIONS; LIMITATIONS.—

1 (i) AVAILABLE TO ALL MEMBERS OF  
2 THE PUBLIC.—For purposes of this para-  
3 graph, information from a website or on-  
4 line service is not available to all members  
5 of the public if the individual to whom the  
6 information pertains has restricted the in-  
7 formation to a specific audience or main-  
8 tained a default setting that restricts the  
9 information to a specific audience.

10 (ii) BUSINESS CONTACT INFORMA-  
11 TION.—The term “publicly available infor-  
12 mation” includes business contact informa-  
13 tion of an individual acting in a business  
14 or professional context that is made avail-  
15 able on a website or online service made  
16 available to all members of the public, in-  
17 cluding the name, position or title, busi-  
18 ness telephone number, business email ad-  
19 dress, or business address of the indi-  
20 vidual.

21 (iii) OTHER LIMITATIONS.—The term  
22 “publicly available information” does not  
23 include—

1 (I) any obscene visual depiction  
2 (as such term is used in section 1460  
3 of title 18, United States Code);

4 (II) derived data from publicly  
5 available information that reveals in-  
6 formation about an individual that  
7 meets the definition of the term “sen-  
8 sitive covered data”;

9 (III) biometric information;

10 (IV) genetic information, unless  
11 made publicly available by the indi-  
12 vidual to whom the information per-  
13 tains by a means described in clause  
14 (ii) or (iii) of subparagraph (A);

15 (V) covered data that is created  
16 through the combination of covered  
17 data with publicly available informa-  
18 tion;

19 (VI) intimate images, authentic  
20 or computer-generated, known to be  
21 nonconsensual; or

22 (VII) sensitive covered data made  
23 available by a data broker.

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

4           (49) SENSITIVE COVERED DATA.—

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

8                   (i) A government-issued identifier, in-  
9                   cluding a Social Security number, passport  
10                  number, or driver’s license number, that is  
11                  not required by law to be displayed in pub-  
12                  lic.

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

18                  (iii) Genetic information.

19                  (iv) A financial account number, debit  
20                  card number, credit card number, or any  
21                  required security or access code, password,  
22                  or credentials allowing access to any such  
23                  account or card, except that the last four  
24                  digits of an account number, debit card

1 number, or credit card number may not be  
2 considered sensitive covered data.

3 (v) Biometric information.

4 (vi) Precise geolocation information.

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

20 (viii) Unencrypted or unredacted ac-  
21 count or device log-in credentials.

22 (ix) Information revealing the sexual  
23 behavior of an individual in a manner in-  
24 consistent with the reasonable expectation

1 of the individual regarding disclosure of  
2 such information.

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

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

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

24 (xiii) Information collected by a cov-  
25 ered entity that is not a provider of a serv-

1           ice described in clause (xii) that reveals the  
2           video content requested or selected by an  
3           individual (excluding any such information  
4           used solely for transfers for independent  
5           video measurement).

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

12          (xv) An online activity profile.

13          (xvi) Information about a covered  
14          minor.

15          (xvii) Information that reveals the sta-  
16          tus of an individual as a member of the  
17          Armed Forces.

18          (xviii) Neural data.

19          (xix) Any other covered data collected,  
20          processed, retained, or transferred for the  
21          purpose of identifying a type of informa-  
22          tion described in any of clauses (i) through  
23          (xviii).



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

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

8 (ii) provides video programming as de-  
9 scribed in such subparagraph.

10 (50) SERVICE PROVIDER.—

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

16 (i) a covered entity or another service  
17 provider; or

18 (ii) a Federal, State, Tribal, or local  
19 government entity.

20 (B) RULE OF CONSTRUCTION.—

21 (i) IN GENERAL.—An entity is a cov-  
22 ered entity and not a service provider with  
23 respect to a specific collecting, processing,  
24 retaining, or transferring of covered data,  
25 if the entity, alone or jointly with others,

1 determines the purposes and means of the  
2 specific collecting, processing, retaining, or  
3 transferring of data.

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

20 (iii) CONTEXT REQUIRED.—Whether  
21 an entity is a covered entity or a service  
22 provider depends on the facts surrounding  
23 how, and the context in which, data is col-  
24 lected, processed, retained, or transferred.

25 (51) SMALL BUSINESS.—

1 (A) IN GENERAL.—The term “small busi-  
2 ness” means an entity (including any affiliate  
3 of the entity)—

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

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

20 (iii) that did not, during the period  
21 described in clause (i), transfer covered  
22 data to a third party in exchange for rev-  
23 enue or anything of value, except for pur-  
24 poses of initiating, rendering, billing for, fi-  
25 nalizing, completing, or otherwise collecting

1 payment for a requested service or product  
2 or facilitating web analytics that are not  
3 used to create an online activity profile.

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

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

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

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

1 (B) any alleged physical or mental harm to  
2 an individual that involves—

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

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

15 (54) TARGETED ADVERTISING.—The term “tar-  
16 geted advertising”—

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

25 (B) includes—

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

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

15 (C) excludes contextual advertising and  
16 first-party advertising.

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

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

21 (A) means any entity that—

22 (i) receives covered data from another  
23 entity that is not the individual to whom  
24 the data pertains; and

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

3 (B) does not include an entity that collects  
4 covered data from another entity if the 2 enti-  
5 ties are—

6 (i) related by common ownership or  
7 corporate control; or

8 (ii) nonprofit entities that are part of  
9 the same federated nonprofit organization.

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

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

19 (59) UNIQUE PERSISTENT IDENTIFIER.—

20 (A) IN GENERAL.—The term “unique per-  
21 sistent identifier” means a technologically cre-  
22 ated identifier to the extent that such identifier  
23 is reasonably linkable to an individual or a de-  
24 vice that identifies or is linked or reasonably  
25 linkable to 1 or more individuals, including de-

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

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

17 (60) WIDELY DISTRIBUTED MEDIA.—

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



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

5 **SEC. 102. DATA MINIMIZATION.**

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

11 (1) to provide or maintain—

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

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

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

24 (b) ADDITIONAL PROTECTIONS FOR SENSITIVE COV-  
25 ERED DATA.—Subject to subsection (a), a covered entity

1 may not transfer sensitive covered data to a third party  
2 or direct a service provider to transfer sensitive covered  
3 data to a third party without the affirmative express con-  
4 sent of the individual to whom such data pertains, unless  
5 for a purpose permitted by paragraph (2), (3), (4), (5),  
6 (6), (8), (9), (11), (12), or (13) of subsection (d).

7 (c) ADDITIONAL PROTECTIONS FOR BIOMETRIC IN-  
8 FORMATION AND GENETIC INFORMATION.—

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

15 (2) PROCESSING.—Subject to subsection (a), a  
16 covered entity may not process biometric information  
17 or genetic information or direct a service provider to  
18 process biometric information or genetic information  
19 without the affirmative express consent of the indi-  
20 vidual to whom such information pertains, unless for  
21 a purpose permitted by paragraph (2), (3), or (4) of  
22 subsection (d).

23 (3) RETENTION.—Subject to subsection (a), a  
24 covered entity may not retain biometric information  
25 or direct a service provider to retain biometric infor-

1       mation beyond the point at which the purpose for  
2       which an individual provided affirmative express  
3       consent under paragraph (1) has been satisfied or  
4       beyond the date that is 3 years after the date of the  
5       last interaction of the individual with the covered en-  
6       tity or service provider, whichever occurs first, un-  
7       less for a purpose permitted under paragraph (2),  
8       (3), or (4) of subsection (d).

9           (4) TRANSFER.—

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

20           (B) NO TRANSFER FOR PAYMENT OR  
21           OTHER VALUABLE CONSIDERATION.—A covered  
22           entity may not transfer biometric information  
23           or genetic information to a third party, or di-  
24           rect a service provider to transfer biometric in-  
25           formation or genetic information to a third

1 party, for payment or other valuable consider-  
2 ation (regardless of the purpose of the transfer,  
3 including a purpose described in subparagraph  
4 (A)).

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

13 (1) To protect data security as described in sec-  
14 tion 109, protect against spam, or protect and main-  
15 tain networks and systems, including through  
16 diagnostics, debugging, and repairs.

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

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

23 (4) To transfer covered data to a Federal,  
24 State, Tribal, or local law enforcement agency pur-

1           suant to a lawful warrant, administrative subpoena,  
2           or other form of lawful process.

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

5           (6) To conduct market research.

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

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

12           (B) conduct research or analytics to im-  
13           prove a product or service of the covered entity  
14           or service provider;

15           (C) conduct research to investigate, estab-  
16           lish, or improve the effectiveness or safety of  
17           medical products, including drugs, biologics,  
18           and medical devices;

19           (D) enable the effective delivery and ad-  
20           ministration of health care products and treat-  
21           ments to patients, in compliance with Federal  
22           regulations; or

23           (E) monitor the safety and efficacy of  
24           health care products and services administered

1 to patients, in compliance with Federal regula-  
2 tions.

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

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

15 (B) a reasonable opportunity to—

16 (i) withdraw any previously provided  
17 consent in accordance with the require-  
18 ments of affirmative express consent under  
19 this title related to the covered data of the  
20 individual; and

21 (ii) request the deletion of the covered  
22 data of the individual, as described in sec-  
23 tion 105.

24 (9) With respect to a covered entity or service  
25 provider that is a telecommunications carrier or a

1 provider of a mobile service, interconnected VoIP  
2 service, or non-interconnected VoIP service (as such  
3 terms are defined in section 3 of the Communica-  
4 tions Act of 1934 (47 U.S.C. 153)), to provide call  
5 location information in a manner described in sub-  
6 paragraph (A) or (C) of section 222(d)(4) of such  
7 Act (47 U.S.C. 222(d)(4)).

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

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

18 (12) To prevent, detect, protect against, inves-  
19 tigate, or respond to an imminent or ongoing public  
20 safety incident (such as a mass casualty event, nat-  
21 ural disaster, or national security incident), exclud-  
22 ing the transfer of covered data for payment or  
23 other valuable consideration to a government entity.

24 (13) Except with respect to health information,  
25 to prevent, detect, protect against, investigate, or re-

1        spond to criminal activity or harassment, excluding  
2        the transfer of covered data for payment or other  
3        valuable consideration to a government entity.

4            (14) Except with respect to sensitive covered  
5        data, and only with respect to covered data pre-  
6        viously collected in accordance with this title, to  
7        process or transfer such data to provide first-party  
8        advertising or contextual advertising or to measure  
9        and report on marketing performance or media per-  
10       performance by the covered entity, including processing  
11       or transferring covered data for measurement and  
12       reporting of frequency, attribution, and performance,  
13       including by independent entities, except that this  
14       paragraph does not permit the processing or trans-  
15       fer of covered data for first-party advertising to a  
16       covered minor as prohibited by section 119.

17           (15) Except with respect to sensitive covered  
18        data, and only with respect to covered data pre-  
19        viously collected in accordance with this title, to  
20        process or transfer such data to provide targeted ad-  
21        vertising, direct mail targeted advertising, or email  
22        targeted advertising (subject to the CAN-SPAM Act  
23        of 2003 (15 U.S.C. 7701 et seq.) and the regula-  
24        tions promulgated under such Act) or to measure  
25        and report on marketing performance or media per-



1 formance, including processing or transferring cov-  
2 ered data for measurement and reporting of fre-  
3 quency, attribution, and performance, including by  
4 independent entities, except that this paragraph does  
5 not permit the processing or transfer of covered data  
6 for targeted advertising to an individual who has  
7 opted out of targeted advertising pursuant to section  
8 106 or to a covered minor as prohibited by section  
9 119.

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

13 (A) is in the public interest;

14 (B) adheres to all relevant laws and regu-  
15 lations governing such research, including regu-  
16 lations for the protection of human subjects, if  
17 applicable;

18 (C) limits transfers to third parties of sen-  
19 sitive covered data to only those transfers nec-  
20 essary, proportionate, and limited to carry out  
21 the research; and

22 (D) prohibits the transfer of covered data  
23 to a data broker.

24 (17) To conduct medical research in compliance  
25 with part 46 of title 45, Code of Federal Regula-

1 tions, or parts 50 and 56 of title 21, Code of Fed-  
2 eral Regulations.

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

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

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

15 (a) IN GENERAL.—Each covered entity and service  
16 provider shall establish, implement, and maintain reason-  
17 able policies, practices, and procedures that reflect the role  
18 of the covered entity or service provider in the collection,  
19 processing, retention, and transferring of covered data.

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

22 (1) identify, assess, and mitigate privacy risks  
23 related to covered minors (including, if applicable, in  
24 a manner that considers the developmental needs of  
25 different age ranges of covered minors), individuals

1 living with disabilities, and individuals over the age  
2 of 65;

3 (2) mitigate privacy risks related to the prod-  
4 ucts and services of the covered entity or service pro-  
5 vider, including in the design, development, and im-  
6 plementation of such products and services, taking  
7 into account the role of the covered entity or service  
8 provider and the information available to the covered  
9 entity or service provider; and

10 (3) implement reasonable internal training and  
11 safeguards to promote compliance with this title and  
12 to mitigate privacy risks, taking into account the  
13 role of the covered entity or service provider and the  
14 information available to the covered entity or service  
15 provider.

16 (c) FACTORS TO CONSIDER.—The policies, practices,  
17 and procedures established by a covered entity or service  
18 provider under subsection (a) shall align with, as applica-  
19 ble—

20 (1) the nature, scope, and complexity of the ac-  
21 tivities engaged in by the covered entity or service  
22 provider, including whether the covered entity or  
23 service provider is a large data holder, nonprofit or-  
24 ganization, or data broker, taking into account the  
25 role of the covered entity or service provider and the

1 information available to the covered entity or service  
2 provider;

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

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

9 (4) the number of individuals and devices to  
10 which the covered data collected, processed, retained,  
11 or transferred by the covered entity or service pro-  
12 vider relates;

13 (5) state-of-the-art administrative, techno-  
14 logical, and organizational measures that, by default,  
15 serve the purpose of protecting the privacy and secu-  
16 rity of covered data as required by this title; and

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

20 (d) COMMISSION GUIDANCE.—Not later than 1 year  
21 after the date of the enactment of this Act, the Commis-  
22 sion shall issue guidance with respect to what constitutes  
23 reasonable policies, practices, and procedures as required  
24 by subsection (a). In issuing such guidance, the Commis-

1 sion shall consider unique circumstances applicable to non-  
2 profit organizations, service providers, and data brokers.

3 **SEC. 104. TRANSPARENCY.**

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

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

13 (1) The identity and the contact information  
14 of—

15 (A) the covered entity or service provider  
16 to which the privacy policy applies, including a  
17 point of contact and a monitored email address  
18 or other monitored online contact mechanism,  
19 as applicable, specific to data privacy and data  
20 security inquiries; and

21 (B) any affiliate within the same corporate  
22 structure as the covered entity or service pro-  
23 vider, to which the covered entity or service pro-  
24 vider may transfer data, that—

1 (i) is not under common branding  
2 with the covered entity or service provider;

3 or

4 (ii) has different contact information  
5 than the covered entity or service provider.

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

8 (A) the categories of covered data the cov-  
9 ered entity or service provider collects, proc-  
10 esses, or retains; and

11 (B) the processing purposes for each such  
12 category of covered data.

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

15 (A) each category of service provider or  
16 third party to which the covered entity or serv-  
17 ice provider transfers covered data;

18 (B) the name of each data broker to which  
19 the covered entity or service provider transfers  
20 covered data; and

21 (C) the purposes for which such data is  
22 transferred.

23 (4) The length of time the covered entity or  
24 service provider intends to retain each category of  
25 covered data or, if it is not possible to identify the

1 length of time, the criteria used to determine the  
2 length of time the covered entity or service provider  
3 intends to retain each category of covered data.

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

7 (6) A description of how the covered entity  
8 treats data collected from covered minors differently  
9 than data collected from other individuals, if the  
10 covered entity has knowledge that the covered entity  
11 has collected data from covered minors.

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

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

15 (9) Whether any covered data collected by the  
16 covered entity or service provider is transferred to,  
17 processed in, retained in, or otherwise accessible to  
18 a foreign adversary (as determined by the Secretary  
19 of Commerce and specified in section 7.4 of title 15,  
20 Code of Federal Regulations (or any successor regu-  
21 lation)).

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

24 (1) in the 10 most-used languages in which a  
25 covered entity or service provider provides products

1 or services or carries out activities related to such  
2 products or services; or

3 (2) if the covered entity or service provider pro-  
4 vides products or services in fewer than 10 lan-  
5 guages, in the languages in which the covered entity  
6 or service provider provides products or services or  
7 carries out activities related to such products or  
8 services.

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

13 (e) MATERIAL CHANGES.—

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

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

19 (i) advance notice of such material  
20 change; and

21 (ii) a means to opt out of the collec-  
22 tion, processing, retention, or transfer of  
23 any covered data of such individual pursu-  
24 ant to such material change; and



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

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

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

23 (f) TRANSPARENCY REQUIREMENTS FOR LARGE  
24 DATA HOLDERS.—

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

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

6           (i) retain and publish on the website  
7 of the large data holder a copy of each  
8 version of the privacy policy of the large  
9 data holder required under subsection (a)  
10 for not less than 10 years; and

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

20           (B) EXCLUSION.—This paragraph does not  
21 apply to material changes to previous versions  
22 of the privacy policy of a large data holder that  
23 precede the date that is 180 days after the date  
24 of the enactment of this Act.

25           (2) SHORT FORM NOTICE TO CONSUMERS.—

1           (A) IN GENERAL.—In addition to the pri-  
2           vacy policy required under subsection (a), a  
3           large data holder shall provide a short-form no-  
4           tice of the covered data practices of the large  
5           data holder in a manner that—

6                   (i) is concise;

7                   (ii) is clear and conspicuous;

8                   (iii) is readily accessible to an indi-  
9           vidual, based on the manner in which the  
10          individual interacts with the large data  
11          holder and the products or services of the  
12          large data holder and what is reasonably  
13          anticipated within the context of the rela-  
14          tionship between the individual and the  
15          large data holder;

16                   (iv) includes an overview of individual  
17          rights and disclosures to reasonably draw  
18          attention to data practices that may be un-  
19          expected or that involve sensitive covered  
20          data; and

21                   (v) is not more than 500 words in  
22          length in the English language or, if in a  
23          language other than English, not more  
24          than 550 words in length.

1 (B) GUIDANCE.—Not later than 180 days  
2 after the date of the enactment of this Act, the  
3 Commission shall issue guidance establishing  
4 the minimum disclosures necessary for the  
5 short-form notice described in this paragraph  
6 and shall include templates or models for such  
7 notice.

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

9 (a) ACCESS TO, AND CORRECTION, DELETION, AND  
10 PORTABILITY OF, COVERED DATA.—After receiving a  
11 verified request from an individual, including a parent act-  
12 ing on behalf of a child of the parent, a covered entity  
13 shall provide the individual with the right to—

14 (1) access—

15 (A) in a format that can be naturally read  
16 by a human, the covered data of the individual  
17 or child (as applicable) (or an accurate rep-  
18 resentation of the covered data of the individual  
19 or child (as applicable), if the covered data is  
20 no longer in the possession of the covered entity  
21 or a service provider acting on behalf of the  
22 covered entity) that is collected, processed, or  
23 retained by the covered entity or any service  
24 provider of the covered entity;

1 (B) the name of any third party or service  
2 provider to whom the covered entity has trans-  
3 ferred the covered data, as well as the cat-  
4 egories of sources from which the covered data  
5 was collected; and

6 (C) a description of the purpose for which  
7 the covered entity transferred any covered data  
8 of the individual or child (as applicable) to a  
9 third party or service provider;

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

20 (3) delete covered data of the individual or child  
21 (as applicable) that is retained by the covered entity  
22 and, for covered data that has been transferred, re-  
23 quest that the covered entity notify any third party  
24 or service provider to which the covered entity trans-  
25 ferred such covered data of the deletion request, in-

1 including so that service providers may provide the as-  
2 sistance required by section 111(a)(1)(C);

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

8 (A) a format that can be naturally read by  
9 a human; and

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

12 (5) delete any content or information submitted  
13 to the covered entity by the individual when a cov-  
14 ered minor and, for any such content or information  
15 that has been transferred, request that the covered  
16 entity notify any third party or service provider to  
17 which the covered entity transferred such content or  
18 information of the deletion request, including so that  
19 service providers may provide the assistance required  
20 by section 111(a)(1)(C).

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

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

25 (2) with respect to—

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

6 (B) any instance beyond the first 3 in-  
7 stances described in subparagraph (A), may  
8 charge a reasonable fee for each additional re-  
9 quest to exercise any such right during such  
10 12-month period.

11 (c) TIMING.—

12 (1) IN GENERAL.—Subject to subsections (b),  
13 (d), and (e), each request under subsection (a) shall  
14 be completed—

15 (A) by any covered entity that is a large  
16 data holder or data broker, not later than 30  
17 calendar days after receiving such request from  
18 an individual, unless it is impossible or demon-  
19 strably impracticable to verify the individual; or

20 (B) by a covered entity that is not a large  
21 data holder or data broker, not later than 45  
22 calendar days after receiving such request from  
23 an individual, unless it is impossible or demon-  
24 strably impracticable to verify the individual.

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

9           (d) VERIFICATION.—

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

13                   (A) the individual whose covered data is  
14                   the subject of the request;

15                   (B) the parent of the child whose covered  
16                   data (or, with respect to a request under sub-  
17                   section (a)(5), whose content or other informa-  
18                   tion) is the subject of the request; or

19                   (C) another individual who is a natural  
20                   person who is authorized to make such a re-  
21                   quest on behalf of the individual whose covered  
22                   data is the subject of the request.

23           (2) ADDITIONAL INFORMATION.—If a covered  
24           entity cannot make the verification described in  
25           paragraph (1), the covered entity may request that



1 the individual making the request provide any addi-  
2 tional information necessary for the sole purpose of  
3 making such verification, except that—

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

6 (B) the covered entity may not process, re-  
7 tain, or transfer such additional information for  
8 any other purpose.

9 (e) EXCEPTIONS.—

10 (1) REQUIRED EXCEPTIONS.—A covered entity  
11 may not permit an individual to exercise a right de-  
12 scribed in subsection (a), in whole or in part, if the  
13 covered entity—

14 (A) cannot reasonably make the  
15 verification described in subsection (d)(1);

16 (B) determines that exercise of the right  
17 would require access to, or the correction or de-  
18 letion of, the sensitive covered data of an indi-  
19 vidual other than the individual whose covered  
20 data is the subject of the request;

21 (C) determines that exercise of the right  
22 would require correction or deletion of covered  
23 data subject to a warrant, lawfully executed  
24 subpoena, or litigation hold notice or equivalent  
25 preservation notice in connection with such war-

1           rant or subpoena or issued in a matter in which  
2           the covered entity is a named party;

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

6           (E) determines that exercise of the right  
7           would violate the professional ethical obligations  
8           of the covered entity;

9           (F) reasonably believes that the request is  
10          made to further fraud;

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

14          (H) reasonably believes that complying  
15          with the request would threaten data security  
16          or network security.

17          (2) PERMISSIVE EXCEPTIONS.—A covered enti-  
18          ty may decline, in whole or in part, to comply with  
19          a request to exercise a right described in subsection  
20          (a), with adequate explanation to the individual  
21          making the request, if compliance with the request  
22          would—

23                 (A) be demonstrably impracticable due to  
24                 technological limitations or prohibitive cost, and  
25                 if the covered entity provides a detailed descrip-

1           tion to the individual regarding the inability to  
2           comply with the request due to technological  
3           limitations or prohibitive cost;

4           (B) delete covered data necessary to per-  
5           form a contract between the covered entity and  
6           the individual;

7           (C) with respect to a right described in  
8           paragraph (1) or (4) of subsection (a), require  
9           the covered entity to release trade secrets or  
10          other privileged, proprietary, or confidential  
11          business information;

12          (D) prevent a covered entity from being  
13          able to maintain a confidential record of opt-out  
14          requests pursuant to this title that is main-  
15          tained solely for the purpose of preventing cov-  
16          ered data of an individual from being collected,  
17          processed, retained, or transferred after the in-  
18          dividual submits an opt-out request;

19          (E) with respect to a deletion request, re-  
20          quire a private elementary or secondary school  
21          (as determined under State law) or a private in-  
22          stitution of higher education (as defined in title  
23          I of the Higher Education Act of 1965 (20  
24          U.S.C. 1001 et seq.)) to delete covered data, if  
25          the deletion would unreasonably interfere with

1 the provision of education services by, or the or-  
2 dinary operation of, the school or institution;

3 (F) delete covered data that relates to a  
4 public figure regarding a matter of legitimate  
5 public interest and for which the requesting in-  
6 dividual has no reasonable expectation of pri-  
7 vacy; or

8 (G) delete covered data that the covered  
9 entity reasonably believes may be evidence of an  
10 abuse of the products or services of the covered  
11 entity, including a violation of terms of service.

12 (3) RULE OF CONSTRUCTION.—This section  
13 may not be construed to require a covered entity or  
14 service provider acting on behalf of a covered entity  
15 to—

16 (A) retain covered data collected for a 1-  
17 time transaction, if such covered data is not  
18 processed or transferred by the covered entity  
19 for any purpose other than completing such  
20 transaction;

21 (B) re-identify, or attempt to re-identify,  
22 de-identified data; or

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

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

6           (5) NUMBER OF REQUESTS.—For purposes of  
7           paragraph (2)(A), the receipt of a large number of  
8           verified requests, on its own, may not be considered  
9           to render compliance with a request demonstrably  
10          impracticable.

11          (6) ADDITIONAL EXCEPTIONS.—

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

22           (B) CONSIDERATIONS.—In establishing  
23           any exceptions under subparagraph (A), the  
24           Commission shall consider any relevant changes  
25           in technology, means for protecting privacy and

1 other rights, and beneficial uses of covered data  
2 by covered entities.

3 (C) CLARIFICATION.—A covered entity  
4 may decline to comply with a request of an in-  
5 dividual to exercise a right under this section  
6 pursuant to an exception the Commission estab-  
7 lishes under this paragraph.

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

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

14 (A) The number of verified access requests  
15 under subsection (a)(1).

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

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

20 (D) The number of verified requests to opt  
21 out of covered data transfers under section  
22 106(a)(1).

23 (E) The number of verified requests to opt  
24 out of targeted advertising under section  
25 106(a)(2).

1 (F) For each category of request described  
2 in subparagraphs (A) through (E), the number  
3 of such requests that the large data holder com-  
4 plied with in whole or in part.

5 (G) For each category of request described  
6 in subparagraphs (A) through (E), the average  
7 number of days within which the large data  
8 holder substantively responded to the requests.

9 (2) PUBLIC DISCLOSURE.—Not later than July  
10 1 of each calendar year, disclose the information  
11 compiled under paragraph (1) for the previous cal-  
12 endar year—

13 (A) in the privacy policy of the large data  
14 holder; or

15 (B) on a publicly available website of the  
16 large data holder that is accessible from a  
17 hyperlink included in the privacy policy.

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

24 (h) ACCESSIBILITY.—

1           (1) LANGUAGE.—A covered entity shall facili-  
2           tate the ability of individuals to make requests to ex-  
3           ercise rights described in subsection (a) in any lan-  
4           guage in which the covered entity provides a product  
5           or service.

6           (2) INDIVIDUALS LIVING WITH DISABILITIES.—  
7           The mechanisms by which a covered entity enables  
8           individuals to make a request to exercise a right de-  
9           scribed in subsection (a) shall be readily accessible  
10          and usable by individuals living with disabilities.

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

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

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

17                       (A) shall provide an individual with a clear  
18                       and conspicuous means to opt out of the trans-  
19                       fer of the covered data of the individual to a  
20                       third party;

21                       (B) upon establishment of an opt out  
22                       mechanism that meets the requirements and  
23                       technical specifications promulgated under sub-  
24                       section (b), shall allow an individual to make an



1 opt-out designation pursuant to subparagraph  
2 (A) through the opt out mechanism;

3 (C) shall abide by an opt-out designation  
4 made pursuant to subparagraph (A) and com-  
5 municate such designation to all relevant serv-  
6 ice providers and third parties; and

7 (D) except as provided in subsection (b) or  
8 (c)(4) of section 102, paragraph (3) or (4) of  
9 section 112(c), or section 119(b), need not  
10 allow an individual to opt out of a transfer of  
11 covered data made pursuant to a permissible  
12 purpose described in paragraph (1), (2), (3),  
13 (4), (5), (6), (7), (8), (9), (10), (11), (12),  
14 (13), or (14) of section 102(d).

15 (2) RIGHT TO OPT OUT OF TARGETED ADVER-  
16 TISING.—A covered entity that engages in targeted  
17 advertising shall—

18 (A) provide an individual with a clear and  
19 conspicuous means to opt out of the processing  
20 and transfer of covered data of the individual in  
21 furtherance of targeted advertising;

22 (B) upon establishment of an opt out  
23 mechanism that meets the requirements and  
24 technical specifications promulgated under sub-  
25 section (b), allow an individual to make an opt-

1 out designation with respect to targeted adver-  
2 tising through the opt-out mechanism; and

3 (C) abide by any such opt-out designation  
4 made by an individual and communicate such  
5 designation to all relevant service providers and  
6 third parties.

7 (b) UNIVERSAL OPT-OUT MECHANISMS.—

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

19 (A) ensures that the opt-out preference  
20 signal—

21 (i) is clearly described, and easy-to-  
22 use by a reasonable individual;

23 (ii) does not require that an individual  
24 provide additional information beyond what  
25 is necessary to indicate such preference;

1 (iii) clearly represents the preference  
2 of an individual;

3 (iv) is provided—

4 (I) in the 10 most-used lan-  
5 guages in which a covered entity pro-  
6 vides products or services subject to  
7 the opt-out; or

8 (II) if the covered entity provides  
9 products or services subject to the  
10 opt-out in fewer than 10 languages, in  
11 the languages in which the covered  
12 entity provides such products or serv-  
13 ices; and

14 (v) is provided in a manner that is  
15 reasonably accessible to and usable by indi-  
16 viduals living with disabilities;

17 (B) provides a mechanism for an individual  
18 to selectively opt out of the collection, proc-  
19 essing, retention, or transfer of covered data by  
20 a covered entity, without affecting the pref-  
21 erences of the individual with respect to other  
22 entities or disabling the opt-out preference sig-  
23 nal globally;

24 (C) states that, in the case of a page or  
25 setting view that the individual accesses to set

1 the opt-out preference signal, the individual  
2 should see up to 2 choices, corresponding to the  
3 rights established under subsection (a); and

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

8 (2) EFFECT OF DESIGNATIONS.—A covered en-  
9 tity shall abide by any designation made by an indi-  
10 vidual through any mechanism that meets the re-  
11 quirements and technical specifications promulgated  
12 under paragraph (1).

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

14 (a) DARK PATTERNS PROHIBITED.—

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

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

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

21 (C) obtain, infer, or facilitate the consent  
22 of an individual for any action that requires the  
23 consent of an individual under this title.

24 (2) CLARIFICATION.—Any agreement by an in-  
25 dividual that is obtained, inferred, or facilitated

1 through dark patterns does not constitute consent  
2 for any purpose under this title.

3 (b) INDIVIDUAL AUTONOMY.—A covered entity may  
4 not condition, effectively condition, attempt to condition,  
5 or attempt to effectively condition the exercise of a right  
6 described in this title through the use of any false, ficti-  
7 tious, fraudulent, or materially misleading statement or  
8 representation.

9 **SEC. 108. PROHIBITION ON DENIAL OF SERVICE AND WAIV-**  
10 **ER OF RIGHTS.**

11 (a) RETALIATION THROUGH SERVICE OR PRICING  
12 PROHIBITED.—A covered entity may not retaliate against  
13 an individual for exercising any of the rights established  
14 under this title, or any regulations promulgated under this  
15 title, including by denying goods or services, charging dif-  
16 ferent prices or rates for goods or services, or providing  
17 a different level of quality of goods or services.

18 (b) RULES OF CONSTRUCTION.—

19 (1) BONA FIDE LOYALTY PROGRAMS.—

20 (A) IN GENERAL.—Nothing in subsection  
21 (a) may be construed to prohibit a covered enti-  
22 ty from offering—

23 (i) to an individual different prices,  
24 rates, levels, qualities, or selections of  
25 goods or services, or functionalities with

1 respect to a product or service, including  
2 offering goods or services for no fee, if the  
3 offering is in connection with the voluntary  
4 participation of the individual in a bona  
5 fide loyalty program, and if—

6 (I) the individual provided af-  
7 firmative express consent to partici-  
8 pate in such bona fide loyalty pro-  
9 gram;

10 (II) the covered entity abides by  
11 the exercise by the individual of any  
12 right provided by subsection (b) or (c)  
13 of section 102, section 105, or section  
14 106; and

15 (III) the sale of covered data is  
16 not a condition of participation in the  
17 bona fide loyalty program; or

18 (ii) to an individual different prices,  
19 rates, levels, qualities, or selections of  
20 goods or services, or functionalities with  
21 respect to a product or service, based on  
22 the decision of the individual to terminate  
23 membership in a bona fide loyalty program  
24 or to exercise a right under section  
25 105(a)(3) to delete covered data that is

1 necessary for participation in the bona fide  
2 loyalty program.

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

6 (i) includes rewards, premium fea-  
7 tures, discounts, and club card programs  
8 offered by a covered entity; and

9 (ii) excludes such programs offered by  
10 a covered high-impact social media com-  
11 pany or data broker.

12 (2) MARKET RESEARCH.—Nothing in sub-  
13 section (a) may be construed to prohibit a covered  
14 entity from offering a financial incentive or other  
15 consideration to an individual for participation in  
16 market research.

17 (3) DECLINING A PRODUCT OR SERVICE.—  
18 Nothing in subsection (a) may be construed to pro-  
19 hibit a covered entity from declining to provide a  
20 product or service or a bona fide loyalty program to  
21 an individual, if any collection, processing, retention,  
22 or transfer affected by the individual exercising a  
23 right established under this title is necessary, pro-  
24 portionate, and limited to providing such product or  
25 service.

1 **SEC. 109. DATA SECURITY AND PROTECTION OF COVERED**  
2 **DATA.**

3 (a) ESTABLISHMENT OF DATA SECURITY PRAC-  
4 TICES.—

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

8 (A) the confidentiality, integrity, and avail-  
9 ability of covered data; and

10 (B) covered data against unauthorized ac-  
11 cess.

12 (2) CONSIDERATIONS.—The data security prac-  
13 tices required under paragraph (1) shall be appro-  
14 priate to—

15 (A) the size and complexity of the covered  
16 entity or service provider;

17 (B) the nature and scope of the relevant  
18 collecting, processing, retaining, or transferring  
19 of covered data, taking into account changing  
20 business operations with respect to covered  
21 data;

22 (C) the volume, nature, and sensitivity of  
23 the covered data; and

24 (D) the state-of-the-art (and limitations  
25 thereof) in administrative, technical, and phys-  
26 ical safeguards for protecting covered data.



1 (b) SPECIFIC REQUIREMENTS.—The data security  
2 practices required under subsection (a) shall include, at  
3 a minimum, the following:

4 (1) ASSESS VULNERABILITIES.—Routinely iden-  
5 tifying and assessing any reasonably foreseeable in-  
6 ternal or external risk to, or vulnerability in, each  
7 system maintained by the covered entity or service  
8 provider that collects, processes, retains, or transfers  
9 covered data, including unauthorized access to or  
10 corruption of such covered data, human  
11 vulnerabilities, access rights, and the use of service  
12 providers. Such activities shall include developing  
13 and implementing a plan for receiving and consid-  
14 ering unsolicited reports of vulnerability by any enti-  
15 ty and, if such a report is reasonably credible, per-  
16 forming a reasonable and timely investigation of  
17 such report and taking appropriate action to protect  
18 covered data against the vulnerability.

19 (2) PREVENTIVE AND CORRECTIVE ACTION.—

20 (A) IN GENERAL.—Taking preventive and  
21 corrective action to mitigate any reasonably  
22 foreseeable internal or external risk to, or vul-  
23 nerability of, covered data identified by the cov-  
24 ered entity or service provider, consistent with  
25 the nature of such risk or vulnerability and the

1           role of the covered entity or service provider in  
2           collecting, processing, retaining, or transferring  
3           the data, which may include implementing ad-  
4           ministrative, technical, or physical safeguards  
5           or changes to data security practices or the ar-  
6           chitecture, installation, or implementation of  
7           network or operating software.

8                   (B) EVALUATION OF PREVENTATIVE AND  
9                   CORRECTIVE ACTION.—Evaluating and making  
10                  reasonable adjustments to the action described  
11                  in subparagraph (A) in light of any material  
12                  changes in state-of-the-art technology, internal  
13                  or external threats to covered data, and chang-  
14                  ing business operations with respect to covered  
15                  data.

16                  (3) INFORMATION RETENTION AND DIS-  
17                  POSAL.—Disposing of covered data (either by or at  
18                  the direction of the covered entity) that is required  
19                  to be deleted by law or is no longer necessary for the  
20                  purpose for which the data was collected, processed,  
21                  retained, or transferred, unless a permitted purpose  
22                  under section 102(d) applies, except that retention  
23                  and disposal of biometric information shall be gov-  
24                  erned by section 102(c)(3). Such disposal shall in-  
25                  clude destroying, permanently erasing, or otherwise

1        modifying the covered data to make such data per-  
2        manently unreadable or indecipherable and unre-  
3        coverable to ensure ongoing compliance with this  
4        section.

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

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

11           (6) INCIDENT RESPONSE.—Implementing pro-  
12       cedures to detect, respond to, and recover from data  
13       security incidents, including breaches.

14        (c) REGULATIONS.—The Commission may, in con-  
15       sultation with the Secretary of Commerce, promulgate, in  
16       accordance with section 553 of title 5, United States Code,  
17       technology-neutral, process-based regulations to carry out  
18       this section.

19        **SEC. 110. EXECUTIVE RESPONSIBILITY.**

20           (a) DESIGNATION OF PRIVACY AND DATA SECURITY  
21       OFFICERS.—

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

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

5                   (A) implement a data privacy program and  
6                   a data security program to safeguard the pri-  
7                   vacy and security of covered data in compliance  
8                   with the requirements of this title; and

9                   (B) facilitate the ongoing compliance of  
10                  the covered entity or service provider with this  
11                  title.

12          (b) REQUIREMENTS FOR LARGE DATA HOLDERS.—

13               (1) DESIGNATION.—A covered entity or service  
14               provider that is a large data holder shall designate  
15               1 qualified employee to serve as a privacy officer and  
16               1 qualified employee to serve as a data security offi-  
17               cer.

18               (2) ANNUAL CERTIFICATION.—

19                   (A) IN GENERAL.—Beginning on the date  
20                   that is 1 year after the date of the enactment  
21                   of this Act, the chief executive officer of a large  
22                   data holder (or, if the large data holder does  
23                   not have a chief executive officer, the highest  
24                   ranking officer of the large data holder) and  
25                   each privacy officer and data security officer of

1 such large data holder designated under para-  
2 graph (1), shall annually certify to the Commis-  
3 sion, in a manner specified by the Commission,  
4 that the large data holder implements and  
5 maintains—

6 (i) internal controls reasonably de-  
7 signed, implemented, maintained, and  
8 monitored to comply with this title; and

9 (ii) internal reporting structures (as  
10 described in paragraph (3)) to ensure that  
11 such certifying officers are involved in, and  
12 responsible for, decisions that impact com-  
13 pliance by the large data holder with this  
14 title.

15 (B) REQUIREMENTS.—A certification sub-  
16 mitted under subparagraph (A) shall be based  
17 on a review of the effectiveness of the internal  
18 controls and reporting structures of the large  
19 data holder that is conducted by the certifying  
20 officers not more than 90 days before the sub-  
21 mission of the certification.

22 (3) INTERNAL REPORTING STRUCTURE RE-  
23 QUIREMENTS.—At least 1 of the officers designated  
24 under paragraph (1) shall, either directly or through  
25 a supervised designee—

1 (A) establish practices to periodically re-  
2 view and update, as necessary, the privacy and  
3 security policies, practices, and procedures of  
4 the large data holder;

5 (B) conduct biennial and comprehensive  
6 audits to ensure the policies, practices, and pro-  
7 cedures of the large data holder comply with  
8 this title and, upon request, make such audits  
9 available to the Commission;

10 (C) develop a program to educate and  
11 train employees about the requirements of this  
12 title;

13 (D) maintain updated, accurate, clear, and  
14 understandable records of all significant privacy  
15 and data security practices of the large data  
16 holder; and

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

20 (4) PRIVACY IMPACT ASSESSMENTS.—

21 (A) IN GENERAL.—Not later than 1 year  
22 after the date of the enactment of this Act or  
23 1 year after the date on which an entity first  
24 meets the definition of the term “large data  
25 holder”, whichever is earlier, and biennially

1           thereafter, each large data holder shall conduct  
2           a privacy impact assessment that weighs the  
3           benefits of the covered data collection, proc-  
4           essing, retention, and transfer practices of the  
5           entity against the potential adverse con-  
6           sequences of such practices to individual pri-  
7           vacy.

8                   (B) ASSESSMENT REQUIREMENTS.—A pri-  
9           vacy impact assessment required under sub-  
10          paragraph (A) shall be—

11                   (i) reasonable and appropriate in  
12          scope given—

13                   (I) the nature and volume of the  
14           covered data collected, processed, re-  
15           tained, or transferred by the large  
16           data holder; and

17                   (II) the potential risks posed to  
18           the privacy of individuals by the col-  
19           lection, processing, retention, and  
20           transfer of covered data by the large  
21           data holder;

22                   (ii) documented in written form and  
23           maintained by the large data holder for as  
24           long as the relevant privacy policy is re-

1           required to be retained under section  
2           104(f)(1); and

3                   (iii) approved by the privacy officer of  
4           the large data holder.

5           (C) ADDITIONAL FACTORS TO INCLUDE IN  
6           ASSESSMENT.—In assessing privacy risks for  
7           purposes of an assessment conducted under  
8           subparagraph (A), including significant risks of  
9           harm to the privacy of an individual or the se-  
10          curity of covered data, the large data holder  
11          shall include reviews of the means by which  
12          technologies, including blockchain and distrib-  
13          uted ledger technologies and other emerging  
14          technologies, including privacy enhancing tech-  
15          nologies, are used to secure covered data.

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

17          (a) SERVICE PROVIDERS.—

18               (1) IN GENERAL.—A service provider that col-  
19          lects, processes, retains, or transfers covered data on  
20          behalf of or at the direction of a covered entity or  
21          another service provider—

22                   (A) shall adhere to the instructions of the  
23          covered entity or other service provider and col-  
24          lect, process, retain, or transfer covered data  
25          only to the extent necessary, proportionate, and



1 limited to provide a service requested by the  
2 covered entity or other service provider, as set  
3 out in the contract described in paragraph (2);

4 (B) may not collect, process, retain, or  
5 transfer covered data if the service provider has  
6 actual knowledge that the covered entity or  
7 other service provider violated this title with re-  
8 spect to such data;

9 (C) shall assist the covered entity or other  
10 service provider in fulfilling the obligations of  
11 the covered entity or other service provider to  
12 respond to consumer rights requests pursuant  
13 to this title by—

14 (i) providing appropriate technical and  
15 organizational support, taking into account  
16 the nature of the processing and the infor-  
17 mation reasonably available to the service  
18 provider; or

19 (ii) fulfilling a request by the covered  
20 entity or other service provider to execute  
21 a consumer rights request that the covered  
22 entity or other service provider has deter-  
23 mined should be compiled with, by either—

24 (I) complying with the request  
25 pursuant to the instructions of the

1 covered entity or other service pro-  
2 vider; or

3 (II) providing written verification  
4 to the covered entity or other service  
5 provider that the service provider does  
6 not hold data related to the request,  
7 that complying with the request would  
8 be inconsistent with the legal obliga-  
9 tions of the service provider, or that  
10 the request falls within an exception  
11 pursuant to this title;

12 (D) shall, upon the reasonable request of  
13 the covered entity or other service provider,  
14 make available to the covered entity or other  
15 service provider all information necessary to  
16 demonstrate the compliance of the service pro-  
17 vider with the requirements of this title;

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

24 (F) may engage another service provider  
25 for purposes of processing or retaining covered

1 data on behalf of the covered entity or other  
2 service provider only after exercising reasonable  
3 care in selecting another service provider as re-  
4 quired by subsection (d), providing the covered  
5 entity or other service provider with written no-  
6 tice of the engagement, and entering into a  
7 written contract that requires the other service  
8 provider to satisfy the requirements of this title  
9 with respect to covered data; and

10 (G) shall—

11 (i) allow and cooperate with reason-  
12 able assessments by the covered entity or  
13 other service provider at least annually; or

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

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

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

9                   (B) shall clearly set forth—

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

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

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

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

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

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

23                   (D) shall prohibit—

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

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

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

15 (b) THIRD PARTIES.—

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

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

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

24 (ii) in the case of sensitive covered  
25 data with respect to which affirmative ex-

1           press consent is not required pursuant to  
2           subsection (b) of section 102, a purpose  
3           for which the covered entity or service pro-  
4           vider made a disclosure pursuant to section  
5           104; or

6           (B) in the case of covered data that is not  
7           sensitive covered data, a purpose for which the  
8           covered entity or service provider made a disclo-  
9           sure pursuant to section 104.

10          (2) CONTRACT REQUIREMENTS.—Before trans-  
11         ferring covered data to a third party, a covered enti-  
12         ty or service provider shall enter into a contract with  
13         the third party that—

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

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

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

22                 (D) requires the third party to notify the  
23                 covered entity or service provider if the third  
24                 party makes a determination that the third

1 party can no longer meet the obligations of the  
2 third party under this title; and

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

8 (c) RULES OF CONSTRUCTION.—

9 (1) SUCCESSIVE ACTOR VIOLATIONS.—

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

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

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

17 (d) REASONABLE CARE.—

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

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



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

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

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

14          (a) NOTICE.—A data broker shall—

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

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

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

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

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

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

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

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

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

11 (A) stalking or harassing an individual; or

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

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

16 (c) DATA BROKER REGISTRATION.—

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

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

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

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

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

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

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

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

23           (3) DATA BROKER REGISTRY.—

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

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

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

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

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

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

20                          (iv) include a mechanism by which an  
21                          individual, including a parent acting on be-  
22                          half of a child of the parent, may submit  
23                          to all registered data brokers a “Delete My  
24                          Data” request that results in registered  
25                          data brokers deleting all covered data re-

1           lated to such individual or child (as appli-  
2           cable) that the data broker did not collect  
3           directly from such individual or when act-  
4           ing as a service provider.

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

8           (4) DO NOT COLLECT AND DELETE MY DATA  
9           REQUESTS.—

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

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

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

1 (ii) the data collected by the data  
2 broker is necessary—

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

5 (II) for the National Center for  
6 Missing and Exploited Children.

7 **SEC. 113. COMMISSION-APPROVED COMPLIANCE GUIDE-**  
8 **LINES.**

9 (a) APPLICATION FOR COMPLIANCE GUIDELINE AP-  
10 PROVAL.—

11 (1) IN GENERAL.—A covered entity that is not  
12 a data broker and is not a large data holder, or a  
13 group of such covered entities, may apply to the  
14 Commission for approval of 1 or more sets of com-  
15 pliance guidelines governing the collection, proc-  
16 essing, retention, or transfer of covered data by the  
17 covered entity or covered entities.

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

20 (A) a description of how the proposed  
21 guidelines will meet or exceed the applicable re-  
22 quirements of this title;

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

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

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

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

12 (3) COMMISSION REVIEW.—

13 (A) INITIAL APPROVAL.—

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

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

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

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

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

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

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



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

4           (B) APPROVAL OF MODIFICATIONS.—

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

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

21          (b) WITHDRAWAL OF APPROVAL.—

22                 (1) IN GENERAL.—If at any time the Commis-  
23          sion determines that guidelines previously approved  
24          under this section no longer meet the applicable re-  
25          quirements of this title or that compliance with the

1 approved guidelines is insufficiently enforced by the  
2 independent organization administering the guide-  
3 lines, the Commission shall notify the relevant cov-  
4 ered entity or group of covered entities and the inde-  
5 pendent organization of the determination of the  
6 Commission to withdraw approval of the guidelines,  
7 including the basis for the determination.

8 (2) OPPORTUNITY TO CURE.—

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

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

23 (c) CERTIFICATION.—A covered entity with guide-  
24 lines approved by the Commission under this section  
25 shall—

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

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

7           (d) **REBUTTABLE PRESUMPTION OF COMPLIANCE.**—  
8           A covered entity that is eligible to participate in guidelines  
9           approved under this section, participates in the guidelines,  
10          and is in compliance with the guidelines shall be entitled  
11          to a rebuttable presumption that the covered entity is in  
12          compliance with the relevant provisions of this title to  
13          which the guidelines apply.

14          (e) **ELIGIBILITY OF SERVICE PROVIDERS.**—This sec-  
15          tion shall apply to a service provider that is not a large  
16          data holder, or a group of such service providers, in the  
17          same manner as this section applies to a covered entity  
18          or group of covered entities. Such a service provider or  
19          group of service providers may apply for approval of, and  
20          participate in, the same guidelines as a covered entity or  
21          group of covered entities.

1 **SEC. 114. PRIVACY-ENHANCING TECHNOLOGY PILOT PRO-**  
2 **GRAM.**

3 (a) PRIVACY-ENHANCING TECHNOLOGY DEFINED.—

4 In this section, the term “privacy-enhancing tech-  
5 nology”—

6 (1) means any software or hardware solution,  
7 cryptographic algorithm, or other technical process  
8 of extracting the value of information without sub-  
9 stantially reducing the privacy and security of the  
10 information; and

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

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

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

24 (1) develop and implement a petition process  
25 for covered entities to request to be a part of the  
26 pilot program; and

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

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

21          (e) REQUIREMENTS.—In carrying out the pilot pro-  
22          gram established under subsection (b), the Commission  
23          shall—

24                (1) receive input from private, public, and aca-  
25                demic stakeholders; and

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

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

11          (g) STUDY REQUIRED.—

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

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

16                   (B) to determine the effectiveness of using  
17                   privacy-enhancing technologies at the Commis-  
18                   sion to support oversight of the data security  
19                   practices of covered entities; and

20                   (C) to develop recommendations to improve  
21                   and advance privacy-enhancing technologies, in-  
22                   cluding by improving communication and co-  
23                   ordination between covered entities and the  
24                   Commission to increase implementation of pri-

1           vacy-enhancing technologies by such entities  
2           and the Commission.

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

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

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

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

18 (j) LIMITATIONS ON LIABILITY.—Any covered entity  
19 that petitions, and is accepted, to be part of the pilot pro-  
20 gram established under subsection (b), actively imple-  
21 ments and maintains the use of privacy-enhancing tech-  
22 nologies, and is determined by the Commission to be in  
23 compliance with the program shall for any action under  
24 section 115 or 116 for a violation of section 109, be  
25 deemed to be in compliance with section 109 with respect



1 to the covered data subject to the privacy-enhancing tech-  
2 nologies.

3 **SEC. 115. ENFORCEMENT BY FEDERAL TRADE COMMIS-**  
4 **SION.**

5 (a) NEW BUREAU.—

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

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

16 (3) STAFF.—

17 (A) IN GENERAL.—In staffing the bureau  
18 established under this subsection, the Commis-  
19 sion shall ensure the allocation of full time em-  
20 ployees or full time employee equivalents that  
21 include attorneys, economists, investigators,  
22 technologists, and mental health professionals  
23 with experience in the well-being of children  
24 and teens.

1           (B) TECHNOLOGIST DEFINED.—For the  
2           purposes of this paragraph, the term “tech-  
3           nologist” means an individual with training and  
4           expertise with respect to technology, including  
5           state-of-the art information technology, network  
6           or data security, hardware or software develop-  
7           ment, privacy-enhancing technologies, cryptog-  
8           raphy, computer science, data science, adver-  
9           tising technology, web tracking, machine learn-  
10          ing, and other related fields and applications.

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

15          (b) ENFORCEMENT BY COMMISSION.—

16           (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-  
17           TICES.—A violation of this title or a regulation pro-  
18           mulgated under this title shall be treated as a viola-  
19           tion of a rule defining an unfair or deceptive act or  
20           practice prescribed under section 18(a)(1)(B) of the  
21           Federal Trade Commission Act (15 U.S.C.  
22           57a(a)(1)(B)).

23           (2) POWERS OF COMMISSION.—

24           (A) IN GENERAL.—Except as provided in  
25           paragraph (3) or otherwise provided in this

1 title, the Commission shall enforce this title and  
2 the regulations promulgated under this title in  
3 the same manner, by the same means, and with  
4 the same jurisdiction, powers, and duties as  
5 though all applicable terms and provisions of  
6 the Federal Trade Commission Act (15 U.S.C.  
7 41 et seq.) were incorporated into and made a  
8 part of this title.

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

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

23 (A) common carriers subject to title II of  
24 the Communications Act of 1934 (47 U.S.C.  
25 201 et seq.); and

1 (B) organizations not organized to carry  
2 on business for their own profit or that of their  
3 members.

4 (4) PENALTY OFFSET FOR STATE ACTIONS.—  
5 Any amount that a court orders an entity to pay in  
6 an action brought under this subsection shall be off-  
7 set by any amount a court has ordered the entity to  
8 pay in an action brought against the entity for the  
9 same violation under section 116.

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

12 (A) ESTABLISHMENT OF VICTIMS RELIEF  
13 FUND.—There is established in the Treasury of  
14 the United States a separate fund to be known  
15 as the “Privacy and Security Victims Relief  
16 Fund” (in this paragraph referred to as the  
17 “Victims Relief Fund”).

18 (B) DEPOSITS.—The Commission or the  
19 Attorney General of the United States, as appli-  
20 cable, shall deposit into the Victims Relief Fund  
21 the amount of any civil penalty obtained in any  
22 civil action the Commission, or the Attorney  
23 General on behalf of the Commission, com-  
24 mences to enforce this title or a regulation pro-  
25 mulgated under this title.

1 (C) USE OF FUND AMOUNTS.—

2 (i) AVAILABILITY TO THE COMMIS-  
3 SION.—Notwithstanding section 3302 of  
4 title 31, United States Code, amounts in  
5 the Victims Relief Fund shall be available  
6 to the Commission, without fiscal year lim-  
7 itation, to provide redress, damages, pay-  
8 ments or compensation, or other monetary  
9 relief to persons affected by an act or prac-  
10 tice for which civil penalties, other mone-  
11 tary relief, or any other forms of relief (in-  
12 cluding injunctive relief) have been ordered  
13 in a civil action or administrative pro-  
14 ceeding the Commission commences, or in  
15 any civil action the Attorney General of the  
16 United States commences on behalf of the  
17 Commission, to enforce this title or a regu-  
18 lation promulgated under this title.

19 (ii) OTHER PERMISSIBLE USES.—To  
20 the extent that individuals cannot be lo-  
21 cated or such redress, damages, payments  
22 or compensation, or other monetary relief  
23 are otherwise not practicable, the Commis-  
24 sion may use amounts in the Victims Re-  
25 lief Fund for the purpose of—

1 (I) consumer or business edu-  
2 cation relating to data privacy or data  
3 security; or

4 (II) engaging in technological re-  
5 search that the Commission considers  
6 necessary to implement this title, in-  
7 cluding promoting privacy-enhancing  
8 technologies that promote compliance  
9 with this title.

10 (D) CALCULATION.—Any amount that the  
11 Commission provides to a person as redress,  
12 payments or compensation, or other monetary  
13 relief under subparagraph (C) with respect to a  
14 violation by an entity shall be offset by any  
15 amount the person received from an action  
16 brought against the entity for the same viola-  
17 tion under section 116.

18 (E) RULE OF CONSTRUCTION.—Amounts  
19 collected and deposited in the Victims Relief  
20 Fund may not be construed to be Government  
21 funds or appropriated monies and may not be  
22 subject to apportionment for the purpose of  
23 chapter 15 of title 31, United States Code, or  
24 under any other authority.

25 (c) REPORT.—

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

7                   (A) the number of such investigations the  
8           Commission commenced;

9                   (B) the number of such investigations the  
10          Commission closed with no official agency ac-  
11          tion;

12                  (C) the disposition of such investigations,  
13          if such investigations have concluded and re-  
14          sulted in official agency action; and

15                  (D) for each investigation that was closed  
16          with no official agency action, the industry sec-  
17          tors of the covered entities subject to each in-  
18          vestigation.

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

23           (3) ANNUAL PLAN.—Not later than 540 days  
24          after the date of the enactment of this Act, and an-  
25          nually thereafter, the Commission shall submit to

1 Congress a plan for the next calendar year describ-  
2 ing the projected activities of the Commission under  
3 this title, including—

4 (A) the policy priorities of the Commission  
5 and any changes to the previous policy prior-  
6 ities of the Commission;

7 (B) any rulemaking proceedings projected  
8 to be commenced, including any such pro-  
9 ceedings to amend or repeal a rule;

10 (C) any plans to develop, update, or with-  
11 draw guidelines or guidance required under this  
12 title;

13 (D) any plans to restructure the Commis-  
14 sion; and

15 (E) projected dates and timelines, or  
16 changes to projected dates and timelines, asso-  
17 ciated with any of the requirements under this  
18 title.

19 **SEC. 116. ENFORCEMENT BY STATES.**

20 (a) CIVIL ACTION.—

21 (1) IN GENERAL.—In any case in which the at-  
22 torney general of a State, the chief consumer protec-  
23 tion officer of a State, or an officer or office of a  
24 State authorized to enforce privacy or data security  
25 laws applicable to covered entities or service pro-



1       viders has reason to believe that an interest of the  
2       residents of the State has been or is adversely af-  
3       fected by the engagement of any entity in an act or  
4       practice that violates this title or a regulation pro-  
5       mulgated under this title, the attorney general, chief  
6       consumer protection officer, or other authorized offi-  
7       cer or office of the State may bring a civil action in  
8       the name of the State, or as *parens patriae* on be-  
9       half of the residents of the State, in an appropriate  
10      Federal district court of the United States to—

11                   (A) enjoin such act or practice;

12                   (B) enforce compliance with this title or  
13      the regulations promulgated under this title;

14                   (C) obtain civil penalties;

15                   (D) obtain damages, restitution, or other  
16      compensation on behalf of the residents of the  
17      State;

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

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

22           (2) LIMITATION.—In any case with respect to  
23      which the attorney general of a State, the chief con-  
24      sumer protection officer of a State, or an officer or  
25      office of a State authorized to enforce privacy or

1 data security laws applicable to covered entities or  
2 service providers brings an action under paragraph  
3 (1), no other officer or office of the same State may  
4 institute a civil action under paragraph (1) against  
5 the same defendant for the same violation of this  
6 title or regulation promulgated under this title.

7 (b) RIGHTS OF THE COMMISSION.—

8 (1) IN GENERAL.—Except if not feasible, a  
9 State officer shall notify the Commission in writing  
10 prior to initiating a civil action under subsection (a).  
11 Such notice shall include a copy of the complaint to  
12 be filed to initiate such action. Upon receiving such  
13 notice, the Commission may intervene in such action  
14 and, upon intervening—

15 (A) be heard on all matters arising in such  
16 action; and

17 (B) file petitions for appeal of a decision in  
18 such action.

19 (2) NOTIFICATION TIMELINE.—If not feasible  
20 for a State officer to provide the notification re-  
21 quired by paragraph (1) before initiating a civil ac-  
22 tion under subsection (a), the State officer shall no-  
23 tify the Commission immediately after initiating the  
24 civil action.

1           (c) ACTIONS BY THE COMMISSION.—In any case in  
2 which a civil action is instituted by or on behalf of the  
3 Commission for a violation of this title or a regulation pro-  
4 mulgated under this title, no attorney general of a State,  
5 chief consumer protection officer of a State, or officer or  
6 office of a State authorized to enforce privacy or data se-  
7 curity laws may, during the pendency of such action, insti-  
8 tute a civil action against any defendant named in the  
9 complaint in the action instituted by or on behalf of the  
10 Commission for a violation of this title or a regulation pro-  
11 mulgated under this title that is alleged in such complaint.

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

21           (e) VENUE; SERVICE OF PROCESS.—

22           (1) VENUE.—Any action brought under sub-  
23 section (a) may be brought in any Federal district  
24 court of the United States that meets applicable re-

1 requirements relating to venue under section 1391 of  
2 title 28, United States Code.

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

6 (A) is an inhabitant; or

7 (B) may be found.

8 (f) GAO STUDY.—

9 (1) IN GENERAL.—The Comptroller General of  
10 the United States shall conduct a study of the prac-  
11 tice of State attorneys general hiring, or otherwise  
12 contracting with, outside firms to assist in enforce-  
13 ment efforts pursuant to this title, which shall in-  
14 clude the study of—

15 (A) the frequency with which each State  
16 attorney general hires or contracts with outside  
17 firms to assist in such enforcement efforts;

18 (B) the contingency fees, hourly rates, and  
19 other costs of hiring or contracting with outside  
20 firms;

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

23 (D) the bid and selection process for such  
24 outside firms, including reviews of conflicts of  
25 interest;

1 (E) the practices State attorneys general  
2 set in place to protect sensitive information that  
3 would become accessible by outside firms while  
4 the outside firms are assisting in such enforce-  
5 ment efforts;

6 (F) the percentage of monetary recovery  
7 that is returned to victims and the percentage  
8 of such recovery that is retained by outside  
9 firms; and

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

12 (2) REPORT.—Not later than 1 year after the  
13 date of the enactment of this Act, the Comptroller  
14 General shall submit to the Committee on Energy  
15 and Commerce of the House of Representatives and  
16 the Committee on Commerce, Science, and Trans-  
17 portation of the Senate a report on the results of the  
18 study conducted under paragraph (1).

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

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

4           (2) exercise the powers conferred on the attor-  
5           ney general, chief consumer protection officer, or of-  
6           ficer or office by the laws of such State, including  
7           the ability to conduct investigations, to administer  
8           oaths or affirmations, or to compel the attendance of  
9           witnesses or the production of documentary or other  
10          evidence.

11          (h) **CALCULATION.**—Any amount that a court orders  
12          an entity to pay to a person under this section shall be  
13          offset by any amount the person received from an action  
14          brought against the entity for the same violation under  
15          section 115.

16          **SEC. 117. RELATION TO OTHER FEDERAL LAWS.**

17          (a) **FEDERAL LAW PRESERVATION.**—

18                 (1) **IN GENERAL.**—Nothing in this title or a  
19                 regulation promulgated under this title may be con-  
20                 strued to limit—

21                         (A) the authority of the Commission, or  
22                         any other Executive agency, under any other  
23                         provision of law;

24                         (B) any requirement for a common carrier  
25                         subject to section 64.2011 of title 47, Code of

1 Federal Regulations (or any successor regula-  
2 tion), regarding information security breaches;  
3 or

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

6 (2) ANTITRUST SAVINGS CLAUSE.—

7 (A) ANTITRUST LAWS DEFINED.—For pur-  
8 poses of this paragraph, the term “antitrust  
9 laws”—

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

13 (ii) includes section 5 of the Federal  
14 Trade Commission Act (15 U.S.C. 45), to  
15 the extent such section applies to unfair  
16 methods of competition.

17 (B) FULL APPLICATION OF THE ANTI-  
18 TRUST LAWS.—Nothing in this title or a regula-  
19 tion promulgated under this title may be con-  
20 strued to modify, impair, supersede the oper-  
21 ation of, or preclude the application of the anti-  
22 trust laws.

23 (3) APPLICATION OF OTHER FEDERAL PRIVACY  
24 AND DATA SECURITY REQUIREMENTS.—

1 (A) IN GENERAL.—To the extent that a  
2 covered entity or service provider is required to  
3 comply with any Federal law or regulation de-  
4 scribed in subparagraph (B), such covered enti-  
5 ty or service provider is not subject to this title  
6 with respect to the activities governed by the re-  
7 quirements of such law or regulation.

8 (B) LAWS AND REGULATIONS DE-  
9 SCRIBED.—The Federal laws and regulations  
10 described in this subparagraph are the fol-  
11 lowing:

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

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

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

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

23 (v) The requirements regarding the  
24 confidentiality of substance use disorder  
25 information under section 543 of the Pub-



1           lic Health Service Act (42 U.S.C. 290dd–  
2           2) or any regulation promulgated under  
3           such section.

4                   (vi) The Fair Credit Reporting Act  
5                   (15 U.S.C. 1681 et seq.).

6                   (vii) Section 444 of the General Edu-  
7                   cation Provisions Act (commonly known as  
8                   the “Family Educational Rights and Pri-  
9                   vacy Act of 1974”) (20 U.S.C. 1232g) and  
10                  part 99 of title 34, Code of Federal Regu-  
11                  lations (or any successor regulation), to  
12                  the extent a covered entity or service pro-  
13                  vider is an educational agency or institu-  
14                  tion (as defined in such section or section  
15                  99.3 of title 34, Code of Federal Regula-  
16                  tions (or any successor regulation)).

17                  (viii) The regulations related to the  
18                  protection of human subjects under part  
19                  46 of title 45, Code of Federal Regula-  
20                  tions.

21                  (x) The Health Care Quality Improve-  
22                  ment Act of 1986 (42 U.S.C. 11101 et  
23                  seq.).

1 (xi) Part C of title IX of the Public  
2 Health Service Act (42 U.S.C. 299b–21 et  
3 seq.).

4 (xii) Chapter 123 of title 18, United  
5 States Code.

6 (C) IMPLEMENTATION GUIDANCE.—Not  
7 later than 1 year after the date of the enact-  
8 ment of this Act, the Commission shall issue  
9 guidance with respect to the implementation of  
10 this paragraph.

11 (b) NONAPPLICATION OF CERTAIN PROVISIONS OF  
12 COMMUNICATIONS ACT OF 1934 AND TELECOMMUNI-  
13 CATIONS ACT OF 1996 RELATED TO FCC PRIVACY AND  
14 DATA SECURITY LAWS AND REGULATIONS.—

15 (1) IN GENERAL.—Except as provided in para-  
16 graph (2), sections 201, 202, 222, 338(i), and 631  
17 of the Communications Act of 1934 (47 U.S.C. 201;  
18 202; 222; 338(i); 551) and section 706 of the Tele-  
19 communications Act of 1996 (47 U.S.C. 1302), and  
20 any regulation or order issued by the Federal Com-  
21 munications Commission under any such section, do  
22 not apply to any covered entity or service provider  
23 with respect to the collection, processing, retention,  
24 transfer, or security of covered data (or the equiva-  
25 lent of such data), to the extent that such sections

1 or any regulation or order issued under such sec-  
2 tions would otherwise cover the collection, proc-  
3 essing, retention, transfer, or security of covered  
4 data (or the equivalent of such data) in order to pro-  
5 tect consumer privacy or the security of such data,  
6 and a covered entity or service provider shall instead  
7 be covered by the requirements of this title with re-  
8 spect to the collection, processing, retention, trans-  
9 fer, and security of covered data.

10 (2) EXCEPTIONS.—Paragraph (1) does not su-  
11 persecede any authority of the Federal Communica-  
12 tions Commission with respect to the following:

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

16 (B) Proceedings to implement section 227  
17 of the Communications Act of 1934 (47 U.S.C.  
18 227) or the Pallone-Thune Telephone Robocall  
19 Abuse Criminal Enforcement and Deterrence  
20 Act (Public Law 116–105; 133 Stat. 3274), or  
21 any other authority used by the Federal Com-  
22 munications Commission to prevent or reduce  
23 unwanted telephone calls or text messages.

24 (C) An enforcement action alleging or find-  
25 ing a violation of a section of the Communica-

1           tions Act of 1934 specified in paragraph (1), if  
2           such action was adopted by the Federal Com-  
3           munications Commission prior to the date of  
4           the enactment of this Act.

5           (D) Subsection (a) of section 222 of the  
6           Communications Act of 1934 (47 U.S.C. 222),  
7           to the extent such subsection imposes a duty on  
8           every telecommunications carrier to protect the  
9           confidentiality of proprietary information of,  
10          and relating to, other telecommunications car-  
11          riers and equipment manufacturers.

12          (E) Subsections (b), (d), and (g) of section  
13          222 of the Communications Act of 1934 (47  
14          U.S.C. 222).

15          (F) Any obligation of an international  
16          treaty related to the exchange of traffic imple-  
17          mented and enforced by the Federal Commu-  
18          nications Commission.

19 **SEC. 118. CHILDREN'S ONLINE PRIVACY PROTECTION ACT**  
20 **OF 1998.**

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

1 **SEC. 119. DATA PROTECTIONS FOR COVERED MINORS.**

2 (a) PROHIBITION ON TARGETED AND FIRST-PARTY  
3 ADVERTISING TO COVERED MINORS.—A covered entity or  
4 service provider acting on behalf of a covered entity may  
5 not engage in targeted advertising or first-party adver-  
6 tising to an individual if the covered entity has knowledge  
7 that the individual is a covered minor, except that a cov-  
8 ered entity or service provider may present or display to  
9 a covered minor age-appropriate advertisements intended  
10 for an audience of covered minors, if the covered entity  
11 or service provider does not use any covered data in rela-  
12 tion to such advertisements, other than data relating to  
13 the status of the individual as a covered minor.

14 (b) DATA TRANSFER REQUIREMENTS RELATED TO  
15 COVERED MINORS.—

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

22 (A) has knowledge that the individual is a  
23 covered minor; and

24 (B) has not obtained affirmative express  
25 consent, unless the transfer is necessary, pro-  
26 portionate, and limited to a purpose expressly

1           permitted by paragraph (2), (3), (4), (8), (9),  
2           (11), (12), or (13) of section 102(d).

3           (2) EXCEPTION.—A covered entity or service  
4           provider may collect, process, retain, or transfer cov-  
5           ered data of an individual that the covered entity or  
6           service provider knows is a covered minor in order  
7           to submit information relating to child victimization  
8           to law enforcement or to the nonprofit, national re-  
9           source center and clearinghouse congressionally des-  
10          ignated to provide assistance to victims, families,  
11          child-serving professionals, and the general public on  
12          missing and exploited children issues.

13          (c) RULEMAKING.—The Commission may conduct a  
14          rulemaking pursuant to section 553 of title 5, United  
15          States Code, to establish processes for parents and teens  
16          to exercise the rights provided in this title with respect  
17          to covered entities and data brokers. Any such rulemaking  
18          shall take into account—

19               (1) the specific needs of parents, children, and  
20               teens;

21               (2) how best to harmonize the processes pro-  
22               vided for under this title with the processes and  
23               guidance provided for under the Children’s Online  
24               Privacy Protection Act of 1998 (15 U.S.C. 6501 et  
25               seq.), as amended by title II of this Act, and any

1 regulations promulgated by the Commission there-  
2 under; and

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

6 **SEC. 120. TERMINATION OF FTC RULEMAKING ON COM-**  
7 **MERCIAL SURVEILLANCE AND DATA SECUR-**  
8 **RITY.**

9 Beginning on the date of the enactment of this Act,  
10 the rulemaking proposed in the advance notice of proposed  
11 rulemaking titled “Trade Regulation Rule on Commercial  
12 Surveillance and Data Security” and published on August  
13 22, 2022 (87 Fed. Reg. 51273) shall be terminated.

14 **SEC. 121. SEVERABILITY.**

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

20 **SEC. 122. INNOVATION RULEMAKINGS.**

21 The Commission may conduct a rulemaking pursuant  
22 to section 553 of title 5, United States Code—

23 (1) to include other covered data in the defini-  
24 tion of the term “sensitive covered data”, except  
25 that the Commission may not expand the category

1 of information described in section 101(49)(A)(ii);  
2 and  
3 (2) to include in the list of permitted purposes  
4 in section 102(d) other permitted purposes for col-  
5 lecting, processing, retaining, or transferring covered  
6 data.

7 **SEC. 123. EFFECTIVE DATE.**

8 Unless otherwise specified in this title, this title shall  
9 take effect on the date that is 180 days after the date  
10 of the enactment of this Act.

11 **TITLE II—CHILDREN’S ONLINE**  
12 **PRIVACY PROTECTION ACT 2.0**

13 **SEC. 201. SHORT TITLE.**

14 This title may be cited as the “Children’s Online Pri-  
15 vacy Protection Act 2.0”.

16 **SEC. 202. ONLINE COLLECTION, USE, DISCLOSURE, AND DE-**  
17 **LETION OF PERSONAL INFORMATION OF**  
18 **CHILDREN.**

19 (a) DEFINITIONS.—Section 1302 of the Children’s  
20 Online Privacy Protection Act of 1998 (15 U.S.C. 6501)  
21 is amended—

22 (1) by amending paragraph (2) to read as fol-  
23 lows:

24 “(2) OPERATOR.—The term ‘operator’—

25 “(A) means any person—



1                   “(i) who, for commercial purposes, in  
2 interstate or foreign commerce, operates or  
3 provides a website on the internet, an on-  
4 line service, an online application, or a mo-  
5 bile application; and

6                   “(ii) who—

7                   “(I) collects or maintains, either  
8 directly or through a service provider,  
9 personal information from or about  
10 the users of that website, service, or  
11 application;

12                   “(II) allows another person to  
13 collect personal information directly  
14 from users of that website, service, or  
15 application (in which case, the oper-  
16 ator is deemed to have collected the  
17 information); or

18                   “(III) allows users of that  
19 website, service, or application to pub-  
20 licly disclose personal information (in  
21 which case, the operator is deemed to  
22 have collected the information); and

23                   “(B) does not include any nonprofit entity  
24 that would otherwise be exempt from coverage

1 under section 5 of the Federal Trade Commis-  
2 sion Act (15 U.S.C. 45).”;

3 (2) in paragraph (4)—

4 (A) by amending subparagraph (A) to read  
5 as follows:

6 “(A) the release of personal information  
7 collected from a child by an operator for any  
8 purpose, except where the personal information  
9 is provided to a person other than an operator  
10 who—

11 “(i) provides support for the internal  
12 operations of a website, online service, on-  
13 line application, or mobile application (as  
14 defined in paragraph (8)(C)) of the oper-  
15 ator, excluding any activity relating to tar-  
16 getted advertising or first-party advertising  
17 (as such terms are defined in section 101  
18 of the American Privacy Rights Act of  
19 2024) to children; and

20 “(ii) does not disclose or use that per-  
21 sonal information for any other purpose;  
22 and”;

23 (B) in subparagraph (B)—

24 (i) by striking “website or online serv-  
25 ices” and inserting “website, online service,

1 online application, or mobile application”;

2 and

3 (ii) by striking “actual knowledge”

4 and inserting “actual knowledge or knowl-

5 edge fairly implied on the basis of objective

6 circumstances”;

7 (3) by striking paragraph (8) and inserting the

8 following:

9 “(8) PERSONAL INFORMATION.—

10 “(A) IN GENERAL.—The term ‘personal in-

11 formation’ means individually identifiable infor-

12 mation about an individual collected online, in-

13 cluding—

14 “(i) a first and last name;

15 “(ii) a home or other physical address

16 including street name and name of a city

17 or town;

18 “(iii) an e-mail address;

19 “(iv) a telephone number;

20 “(v) a Social Security number;

21 “(vi) any other identifier that the

22 Commission determines permits the phys-

23 ical or online contacting of a specific indi-

24 vidual;

1           “(vii) a persistent identifier that can  
2           be used to recognize a specific child over  
3           time and across different websites, online  
4           services, online applications, or mobile ap-  
5           plications, including a customer number  
6           held in a cookie, an Internet Protocol (IP)  
7           address, a processor or device serial num-  
8           ber, or a unique device identifier, but ex-  
9           cluding an identifier that is used by an op-  
10          erator solely for providing support for the  
11          internal operations of a website, online  
12          service, online application, or mobile appli-  
13          cation;

14           “(viii) a photograph, video, or audio  
15          file, if such file contains the image or voice  
16          of a specific child;

17           “(ix) geolocation information;

18           “(x) information generated from the  
19          measurement or technological processing of  
20          the biological, physical, or physiological  
21          characteristics of an individual that is used  
22          to identify an individual, including—

23                   “(I) fingerprints;

24                   “(II) voice prints;

1                   “(III) iris or retina imagery  
2                   scans;

3                   “(IV) facial templates;

4                   “(V) deoxyribonucleic acid  
5                   (DNA) information; or

6                   “(VI) gait; or

7                   “(xi) information linked or reasonably  
8                   linkable to a child or the parents of that  
9                   child (including any unique identifier) that  
10                  an operator collects online from the child  
11                  and combines with an identifier described  
12                  in this subparagraph.

13                  “(B) EXCLUSION.—The term ‘personal in-  
14                  formation’ does not include an audio file that  
15                  contains the voice of a child, if the operator—

16                   “(i) does not request information via  
17                   voice that would otherwise be considered  
18                   personal information under this paragraph;

19                   “(ii) provides, in the privacy policy of  
20                   the operator, clear notice of the collection  
21                   and use of the audio file by the operator  
22                   and the deletion policy of the operator;

23                   “(iii) uses the voice within the audio  
24                   file solely as a replacement for written  
25                   words, to perform a task, or to engage

1 with a website, online service, online appli-  
2 cation, or mobile application, such as to  
3 perform a search or fulfill a verbal instruc-  
4 tion or request; and

5 “(iv) only maintains the audio file  
6 long enough to complete the stated purpose  
7 and then immediately deletes the audio file  
8 and does not make any other use of the  
9 audio file prior to deletion.

10 “(C) SUPPORT FOR THE INTERNAL OPER-  
11 ATIONS OF A WEBSITE, ONLINE SERVICE, ON-  
12 LINE APPLICATION, OR MOBILE APPLICATION.—

13 “(i) IN GENERAL.—For purposes of  
14 subparagraph (A)(vii), the term ‘support  
15 for the internal operations of a website, on-  
16 line service, online application, or mobile  
17 application’ means those activities nec-  
18 essary to—

19 “(I) maintain or analyze the  
20 functioning of the website, online serv-  
21 ice, online application, or mobile appli-  
22 cation;

23 “(II) perform network commu-  
24 nications;

1                   “(III) authenticate users of, or  
2                   personalize the content on, the  
3                   website, online service, online applica-  
4                   tion, or mobile application;

5                   “(IV) cap the frequency of adver-  
6                   tising;

7                   “(V) protect the security or in-  
8                   tegrity of the user, website, online  
9                   service, online application, or mobile  
10                  application;

11                  “(VI) ensure legal or regulatory  
12                  compliance; or

13                  “(VII) fulfill a request of a child  
14                  as permitted by subparagraphs (A)  
15                  through (C) of section 1303(b)(2).

16                  “(ii) CONDITION.—Except as specifi-  
17                  cally permitted under clause (i), informa-  
18                  tion collected for the activities listed in  
19                  clause (i) may not be used or disclosed to  
20                  contact a specific individual, including  
21                  through targeted advertising or first-party  
22                  advertising (as such terms are defined in  
23                  section 101 of the American Privacy  
24                  Rights Act of 2024) to children, to amass  
25                  a profile on a specific individual, in connec-

1           tion with processes that encourage or  
2           prompt use of a website, online service, on-  
3           line application, or mobile application, or  
4           for any other purpose.”;

5           (4) by amending paragraph (9) to read as fol-  
6           lows:

7           “(9) VERIFIABLE CONSENT.—The term  
8           ‘verifiable consent’ means any reasonable effort (tak-  
9           ing into consideration available technology), includ-  
10          ing a request for authorization for future collection,  
11          use, and disclosure described in the notice, to ensure  
12          that a parent of the child—

13                 “(A) receives direct notice of the personal  
14                 information collection, use, and disclosure prac-  
15                 tices of the operator; and

16                 “(B) before the personal information of the  
17                 child is collected, freely and unambiguously au-  
18                 thorizes—

19                         “(i) the collection, use, and disclosure,  
20                         as applicable, of that personal information;  
21                         and

22                         “(ii) any subsequent use of that per-  
23                         sonal information.”;

24           (5) in paragraph (10)—



1 (A) in the paragraph heading, by striking  
2 “WEBSITE OR ONLINE SERVICE DIRECTED TO  
3 CHILDREN” and inserting “WEBSITE, ONLINE  
4 SERVICE, ONLINE APPLICATION, OR MOBILE AP-  
5 PPLICATION DIRECTED TO CHILDREN”;

6 (B) by striking “website or online service”  
7 each place it appears and inserting “website,  
8 online service, online application, or mobile ap-  
9 plication”; and

10 (C) by adding at the end the following new  
11 subparagraph:

12 “(C) RULE OF CONSTRUCTION.—In con-  
13 sidering whether a website, online service, on-  
14 line application, or mobile application, or por-  
15 tion thereof, is directed to children, the Com-  
16 mission shall apply a totality of circumstances  
17 test and shall also consider competent and reli-  
18 able empirical evidence regarding audience com-  
19 position and evidence regarding the intended  
20 audience of the website, online service, online  
21 application, or mobile application.”; and

22 (6) by adding at the end the following:

23 “(13) CONNECTED DEVICE.—The term ‘con-  
24 nected device’ has the meaning given such term in

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

3 “(14) EDUCATIONAL AGENCY OR INSTITU-  
4 TION.—The term ‘educational agency or institution’  
5 means a State educational agency or local edu-  
6 cational agency as defined under Federal law, as  
7 well as an institutional day or residential school, in-  
8 cluding a public school, charter school, or private  
9 school, that provides elementary or secondary edu-  
10 cation, as determined under State law.

11 “(15) MOBILE APPLICATION.—The term ‘mo-  
12 bile application’ has the meaning given such term in  
13 section 101 of the American Privacy Rights Act of  
14 2024.

15 “(16) ONLINE APPLICATION.—The term ‘online  
16 application’ has the meaning given such term in sec-  
17 tion 101 of the American Privacy Rights Act of  
18 2024.

19 “(17) PRECISE GEOLOCATION INFORMATION.—  
20 The term ‘precise geolocation information’ has the  
21 meaning given such term in section 101 of the  
22 American Privacy Rights Act of 2024.”.

23 (b) ONLINE COLLECTION, USE, DISCLOSURE, AND  
24 DELETION OF PERSONAL INFORMATION OF CHILDREN.—

1 Section 1303 of the Children’s Online Privacy Protection  
2 Act of 1998 (15 U.S.C. 6502) is amended—

3 (1) by striking the heading and inserting the  
4 following: “**ONLINE COLLECTION, USE, DISCLO-**  
5 **SURE, AND DELETION OF PERSONAL INFORMA-**  
6 **TION OF CHILDREN.**” ;

7 (2) by amending subsection (a) to read as fol-  
8 lows:

9 “(a) ACTS PROHIBITED.—It is unlawful for an oper-  
10 ator of a website, online service, online application, or mo-  
11 bile application directed to children or for any operator  
12 of a website, online service, online application, or mobile  
13 application with actual knowledge or knowledge fairly im-  
14 plied on the basis of objective circumstances that a user  
15 is a child—

16 “(1) to collect personal information from a child  
17 in a manner that violates the American Privacy  
18 Rights Act of 2024 or the regulations prescribed  
19 under subsection (b); or

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

22 “(A) the operator provides direct notice to  
23 the parent of the child that the personal infor-  
24 mation of the child is being stored or trans-  
25 ferred outside of the United States; and

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

4           (3) in subsection (b)—

5                 (A) in paragraph (1)—

6                     (i) in subparagraph (A)—

7                             (I) in the matter preceding clause  
8                             (i), by striking “operator of any  
9                             website” and all that follows through  
10                            “from a child” and inserting “oper-  
11                            ator of a website, online service, on-  
12                            line application, or mobile application  
13                            directed to children or that has actual  
14                            knowledge or knowledge fairly implied  
15                            on the basis of objective circumstances  
16                            that a user is a child”;

17                            (II) in clause (i)—

18                                 (aa) by striking “notice on  
19                                 the website” and inserting “clear  
20                                 and conspicuous notice on the  
21                                 website, service, or application”;  
22                                 and

23                                 (bb) by striking “; and” and  
24                                 inserting a semicolon;

25                            (III) in clause (ii)—

1 (aa) by striking “verifiable  
2 parental consent” and inserting  
3 “verifiable consent”; and

4 (bb) by striking the semi-  
5 colon at the end and inserting “;  
6 and”; and

7 (IV) by inserting after clause (ii)  
8 the following new clause:

9 “(iii) to obtain verifiable consent from  
10 a parent of a child before using or dis-  
11 closing personal information of the child  
12 for any purpose that is a material change  
13 from the original purposes and disclosure  
14 practices specified to the parent of the  
15 child under clause (i);”;

16 (ii) by striking subparagraph (B);

17 (iii) in subparagraph (C)—

18 (I) by striking “reasonably”; and

19 (II) by inserting “, proportionate,  
20 and limited” after “necessary”;

21 (iv) in subparagraph (D), by striking  
22 “website or online service” and inserting  
23 “website, online service, online application,  
24 or mobile application”; and

1 (v) by redesignating subparagraphs  
2 (C) and (D) as subparagraphs (B) and  
3 (C), respectively;

4 (B) in paragraph (2)—

5 (i) in the matter preceding subpara-  
6 graph (A)—

7 (I) by striking “verifiable paren-  
8 tal consent” and inserting “verifiable  
9 consent”; and

10 (II) by striking “paragraph  
11 (1)(A)(ii)” and inserting “clause (ii)  
12 or (iii) of paragraph (1)(A)”;

13 (ii) in subparagraph (A), by inserting  
14 “or to contact another child” after “to re-  
15 contact the child”;

16 (iii) in subparagraph (B)—

17 (I) by striking “or child”; and

18 (II) by striking “parental con-  
19 sent” each place the term appears and  
20 inserting “verifiable consent”;

21 (iv) in subparagraph (D), in the mat-  
22 ter preceding clause (i)—

23 (I) by striking “reasonably”; and

24 (II) by inserting “, proportionate,  
25 and limited” after “necessary”; and

1 (v) in subparagraph (E)—

2 (I) in the matter preceding clause  
3 (i), by striking “website or online  
4 service” and inserting “website, online  
5 service, online application, or mobile  
6 application”; and

7 (II) in clause (i), by striking  
8 “website” and inserting “website,  
9 service, or application”;

10 (C) by redesignating paragraph (3) as  
11 paragraph (4) and inserting after paragraph  
12 (2) the following new paragraph:

13 “(3) APPLICATION TO OPERATORS ACTING  
14 UNDER AGREEMENTS WITH EDUCATIONAL AGENCIES  
15 OR INSTITUTIONS.—The regulations may provide  
16 that verifiable consent under clause (ii) or (iii) of  
17 paragraph (1)(A) is not required for an operator  
18 that is acting under a written agreement with an  
19 educational agency or institution that, at a min-  
20 imum, requires—

21 “(A) the operator to—

22 “(i) limit its collection, use, and dis-  
23 closure of the personal information from a  
24 child to solely educational purposes and for  
25 no other commercial purposes;

1           “(ii) provide the educational agency or  
2           institution with a notice of the specific  
3           types of personal information the operator  
4           will collect from the child, the method by  
5           which the operator will obtain the personal  
6           information, and the purposes for which  
7           the operator will collect, use, disclose, and  
8           retain the personal information;

9           “(iii) provide the educational agency  
10          or institution with a link to the online no-  
11          tice of information practices of the oper-  
12          ator as required under paragraph  
13          (1)(A)(i); and

14          “(iv) provide the educational agency  
15          or institution, upon request, with a means  
16          to review the personal information collected  
17          from a child, to prevent further use or  
18          maintenance or future collection of per-  
19          sonal information from a child, and to de-  
20          lete personal information collected from a  
21          child or content or information submitted  
22          by a child to the website, online service,  
23          online application, or mobile application of  
24          the operator;



1           “(B) a representative of the educational  
2 agency or institution to—

3           “(i) acknowledge and agree that the  
4 representative has authority to authorize  
5 the collection, use, and disclosure of per-  
6 sonal information from children on behalf  
7 of the educational agency or institution;  
8 and

9           “(ii) provide the name of the rep-  
10 resentative and the title of the representa-  
11 tive at the educational agency or institu-  
12 tion; and

13           “(C) the educational agency or institution  
14 to—

15           “(i) provide on the website of the edu-  
16 cational agency or institution a notice that  
17 identifies the operator with which the edu-  
18 cational agency or institution has entered  
19 into a written agreement under this para-  
20 graph and a link to the online notice of in-  
21 formation practices of the operator as re-  
22 quired under paragraph (1)(A)(i);

23           “(ii) provide the notice of the operator  
24 regarding the information practices of the

1 operator, as required under subparagraph  
2 (A)(ii), upon request, to a parent; and

3 “(iii) upon the request of a parent, re-  
4 quest the operator provide a means to re-  
5 view the personal information collected  
6 from the child of the parent and provide  
7 the parent a means to review the personal  
8 information.”;

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

11 “(4) TERMINATION OF SERVICE.—The regula-  
12 tions shall permit the operator of a website, online  
13 service, online application, or mobile application to  
14 terminate service provided to a child whose parent  
15 has requested to delete covered data of the child  
16 pursuant to section 105 of the American Privacy  
17 Rights Act of 2024.”; and

18 (E) by adding at the end the following new  
19 paragraphs:

20 “(5) CONTINUATION OF SERVICE.—The regula-  
21 tions shall prohibit an operator from discontinuing  
22 service provided to a child on the basis of a request  
23 by the parent of the child to delete personal informa-  
24 tion collected from the child, to the extent that the

1 operator is capable of providing such service without  
2 such information.

3 “(6) COMMON VERIFIABLE CONSENT MECHA-  
4 NISM.—

5 “(A) IN GENERAL.—

6 “(i) FEASIBILITY OF MECHANISM.—

7 The Commission shall conduct an assess-  
8 ment, with notice and public comment, of  
9 the feasibility of allowing operators the op-  
10 tion to use a common verifiable consent  
11 mechanism that fully meets the require-  
12 ments of this title.

13 “(ii) REQUIREMENTS.—The feasibility  
14 assessment described in clause (i) shall  
15 consider whether a single operator could  
16 use a common verifiable consent mecha-  
17 nism to obtain verifiable consent, as re-  
18 quired under this title, from a parent of a  
19 child on behalf of multiple, listed operators  
20 that provide a joint or related service.

21 “(B) REPORT.—Not later than 1 year  
22 after the date of the enactment of this para-  
23 graph, the Commission shall submit to the  
24 Committee on Commerce, Science, and Trans-  
25 portation of the Senate and the Committee on

1 Energy and Commerce of the House of Rep-  
2 resentatives a report with the findings of the  
3 assessment required by subparagraph (A).

4 “(C) REGULATIONS.—If the Commission  
5 finds, in the assessment required by subpara-  
6 graph (A), that the use of a common verifiable  
7 consent mechanism is feasible and would meet  
8 the requirements of this title, the Commission  
9 shall issue regulations, pursuant to section 553  
10 of title 5, United States Code, to permit the use  
11 of a common verifiable consent mechanism in  
12 accordance with the findings outlined in the re-  
13 port submitted under subparagraph (B).”;

14 (4) in subsection (c), by striking “a regulation  
15 prescribed under subsection (a)” and inserting  
16 “paragraph (2) of subsection (a), or of a regulation  
17 prescribed under subsection (b),”; and

18 (5) by striking subsection (d) and inserting the  
19 following:

20 “(d) RELATIONSHIP TO STATE LAW.—The provisions  
21 of this title shall preempt any State law, rule, or regula-  
22 tion only to the extent that such State law, rule, or regula-  
23 tion conflicts with a provision of this title. Nothing in this  
24 title may be construed to prohibit any State from enacting

1 a law, rule, or regulation that provides greater protection  
2 to children than the provisions of this title.”.

3 (c) SAFE HARBORS.—Section 1304 of the Children’s  
4 Online Privacy Protection Act of 1998 (15 U.S.C. 6503)  
5 is amended by adding at the end the following:

6 “(d) PUBLICATION.—

7 “(1) IN GENERAL.—Subject to the restrictions  
8 described in paragraph (2), the Commission shall  
9 publish on the website of the Commission any report  
10 or documentation required by regulation to be sub-  
11 mitted to the Commission to carry out this section.

12 “(2) RESTRICTIONS ON PUBLICATION.—The re-  
13 strictions described in sections 6(f) and 21 of the  
14 Federal Trade Commission Act (15 U.S.C. 46(f);  
15 57b–2) applicable to the disclosure of information  
16 obtained by the Commission shall apply in the same  
17 manner to the disclosure under this subsection of in-  
18 formation obtained by the Commission from a report  
19 or documentation described in paragraph (1).”.

20 (d) ACTIONS BY STATES.—Section 1305 of the Chil-  
21 dren’s Online Privacy Protection Act of 1998 (15 U.S.C.  
22 6504) is amended—

23 (1) in subsection (a)(1)—

1 (A) in the matter preceding subparagraph  
2 (A), by inserting “section 1303(a) or” before  
3 “any regulation”; and

4 (B) in subparagraph (B), by striking “the  
5 regulation” and inserting “such section or regu-  
6 lation”; and

7 (2) in subsection (d)—

8 (A) by inserting “section 1303(a) or” be-  
9 fore “any regulation”; and

10 (B) by striking “that regulation” and in-  
11 serting “such section or regulation”.

12 (e) ADMINISTRATION AND APPLICABILITY OF ACT.—

13 Section 1306 of the Children’s Online Privacy Protection  
14 Act of 1998 (15 U.S.C. 6505) is amended—

15 (1) in subsection (d)—

16 (A) by inserting “section 1303(a) or” be-  
17 fore “a rule”; and

18 (B) by striking “such rule” and inserting  
19 “section 1303(a) or a rule of the Commission  
20 under section 1303”; and

21 (2) by adding at the end the following new sub-  
22 sections:

23 “(f) DETERMINATION OF WHETHER AN OPERATOR  
24 HAS KNOWLEDGE FAIRLY IMPLIED ON THE BASIS OF  
25 OBJECTIVE CIRCUMSTANCES.—

1           “(1) RULE OF CONSTRUCTION.—For purposes  
2 of enforcing this title or a regulation promulgated  
3 under this title, in making a determination as to  
4 whether an operator has knowledge fairly implied on  
5 the basis of objective circumstances that a specific  
6 user is a child, the Commission or a State attorney  
7 general shall rely on competent and reliable evi-  
8 dence, taking into account the totality of the cir-  
9 cumstances, including whether a reasonable and pru-  
10 dent person under the circumstances would have  
11 known that the user is a child. Nothing in this title,  
12 including a determination described in the preceding  
13 sentence, may be construed to require an operator  
14 to—

15           “(A) affirmatively collect any personal in-  
16 formation with respect to the age of a child that  
17 an operator is not already collecting in the nor-  
18 mal course of business; or

19           “(B) implement an age gating or age  
20 verification functionality.

21           “(2) COMMISSION GUIDANCE.—

22           “(A) IN GENERAL.—Not later than 180  
23 days after the date of the enactment of this  
24 subsection, the Commission shall issue guidance  
25 to provide information, including best practices

1 and examples, for operators to understand the  
2 process of the Commission for determining  
3 whether an operator has knowledge fairly im-  
4 plied on the basis of objective circumstances  
5 that a user is a child.

6 “(B) LIMITATION.—No guidance issued by  
7 the Commission under subparagraph (A) con-  
8 fers any rights on any person, State, or locality,  
9 or operates to bind the Commission or any per-  
10 son, State, or locality to the approach rec-  
11 ommended in such guidance. In any enforce-  
12 ment action brought pursuant to this title, the  
13 Commission or State attorney general, as appli-  
14 cable, shall allege a specific violation of a provi-  
15 sion of this title, and the Commission or State  
16 attorney general, as applicable, may not base an  
17 enforcement action on, or execute a consent  
18 order based on, practices that are alleged to be  
19 inconsistent with any such guidance, unless the  
20 practices allegedly violate this title.

21 “(g) ADDITIONAL REQUIREMENT.—Any regulations  
22 issued under this title shall include a description and anal-  
23 ysis of the impact of proposed and final rules on small  
24 entities per chapter 6 of title 5, United States Code.”.



1 **SEC. 203. STUDY AND REPORTS ON MOBILE AND ONLINE**  
2 **APPLICATION OVERSIGHT AND ENFORCE-**  
3 **MENT.**

4 (a) OVERSIGHT REPORT.—Not later than 3 years  
5 after the date of the enactment of this Act, the Federal  
6 Trade Commission shall submit to the Committee on Com-  
7 merce, Science, and Transportation of the Senate and the  
8 Committee on Energy and Commerce of the House of  
9 Representatives a report on the processes of platforms  
10 that offer mobile and online applications for ensuring that,  
11 for those applications that are websites, online services,  
12 online applications, or mobile applications directed to chil-  
13 dren, the applications operate in accordance with—

14 (1) this title, the amendments made by this  
15 title, and any rules promulgated under this title or  
16 the amendments made by this title; and

17 (2) rules promulgated by the Commission under  
18 section 18 of the Federal Trade Commission Act (15  
19 U.S.C. 57a) relating to unfair or deceptive acts or  
20 practices in marketing.

21 (b) ENFORCEMENT REPORT.—Not later than 1 year  
22 after the date of the enactment of this Act, and annually  
23 thereafter, the Federal Trade Commission shall submit to  
24 the Committee on Commerce, Science, and Transportation  
25 of the Senate and the Committee on Energy and Com-

1 merce of the House of Representatives a report that ad-  
2 dresses, at a minimum—

3 (1) the number of actions brought by the Com-  
4 mission during the reporting year to enforce the  
5 Children’s Online Privacy Protection Act of 1998  
6 (15 U.S.C. 6501 et seq.) and the outcome of each  
7 such action;

8 (2) the total number of investigations or inquir-  
9 ies into potential violations of such Act commenced  
10 during the reporting year;

11 (3) the total number of open investigations or  
12 inquiries into potential violations of such Act as of  
13 the time the report is submitted;

14 (4) the number and nature of complaints re-  
15 ceived by the Commission relating to an allegation  
16 of a violation of such Act during the reporting year;  
17 and

18 (5) policy or legislative recommendations to  
19 strengthen online protections for children.

20 (c) REPORT BY THE INSPECTOR GENERAL.—

21 (1) IN GENERAL.—Not later than 2 years after  
22 the date of the enactment of this Act, the Inspector  
23 General of the Federal Trade Commission shall sub-  
24 mit to the Federal Trade Commission and to the  
25 Committee on Commerce, Science, and Transpor-

1 tation of the Senate and the Committee on Energy  
2 and Commerce of the House of Representatives a re-  
3 port regarding the safe harbor provisions in section  
4 1304 of the Children’s Online Privacy Protection  
5 Act of 1998 (15 U.S.C. 6503), which shall include—

6 (A) an analysis of whether the safe harbor  
7 provisions are—

8 (i) operating fairly and effectively;

9 and

10 (ii) effectively protecting the interests  
11 of children; and

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

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

19 **SEC. 204. SEVERABILITY.**

20 If any provision of this title or the amendments made  
21 by this title, or the application thereof to any person or  
22 circumstance, is held invalid, the remainder of this title  
23 and the amendments made by this title, and the applica-  
24 tion of such provision to other persons not similarly situ-

1 ated or to other circumstances, may not be affected by  
2 the invalidation.

