

## Union Calendar No.

117<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

# H. R. 8152

[Report No. 117-]

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

---

### IN THE HOUSE OF REPRESENTATIVES

JUNE 21, 2022

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

JULY --, 2022

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in italics]

[For text of introduced bill, see copy of bill as introduced on June 21, 2022]

# **A BILL**

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

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

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

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

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

*Sec. 1. Short title; table of contents.*

*Sec. 2. Definitions.*

**TITLE I—DUTY OF LOYALTY**

*Sec. 101. Data minimization.*

*Sec. 102. Loyalty duties.*

*Sec. 103. Privacy by design.*

*Sec. 104. Loyalty to individuals with respect to pricing.*

**TITLE II—CONSUMER DATA RIGHTS**

*Sec. 201. Consumer awareness.*

*Sec. 202. Transparency.*

*Sec. 203. Individual data ownership and control.*

*Sec. 204. Right to consent and object.*

*Sec. 205. Data protections for children and minors.*

*Sec. 206. Third-party collecting entities.*

*Sec. 207. Civil rights and algorithms.*

*Sec. 208. Data security and protection of covered data.*

*Sec. 209. Small business protections.*

*Sec. 210. Unified opt-out mechanisms.*

**TITLE III—CORPORATE ACCOUNTABILITY**

*Sec. 301. Executive responsibility.*

*Sec. 302. Service providers and third parties.*

*Sec. 303. Technical compliance programs.*

*Sec. 304. Commission approved compliance guidelines.*

*Sec. 305. Digital content forgeries.*

**TITLE IV—ENFORCEMENT, APPLICABILITY, AND MISCELLANEOUS**

*Sec. 401. Enforcement by the Federal Trade Commission.*

*Sec. 402. Enforcement by States.*

*Sec. 403. Enforcement by persons.*

*Sec. 404. Relationship to Federal and State laws.*

*Sec. 405. Severability.*

*Sec. 406. COPPA.*

*Sec. 407. Authorization of appropriations.*

*Sec. 408. Effective date.*

1 **SEC. 2. DEFINITIONS.**

2 *In this Act:*

3 (1) *AFFIRMATIVE EXPRESS CONSENT.—*

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

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

16 (i) *The request is provided to the indi-*  
17 *vidual in a clear and conspicuous stand-*  
18 *alone disclosure made through the primary*  
19 *medium used to offer the covered entity’s*  
20 *product or service, or only if the product or*  
21 *service is not offered in a medium that per-*  
22 *mits the making of the request under this*  
23 *paragraph, another medium regularly used*  
24 *in conjunction with the covered entity’s*  
25 *product or service.*

1                   (ii) *The request includes a description*  
2 *of the processing purpose for which the indi-*  
3 *vidual's consent is sought and—*

4                   (I) *clearly states the specific cat-*  
5 *egories of covered data that the covered*  
6 *entity shall collect, process, and trans-*  
7 *fer necessary to effectuate the proc-*  
8 *essing purpose; and*

9                   (II) *includes a prominent heading*  
10 *and is written in easy-to-understand*  
11 *language that would enable a reason-*  
12 *able individual to identify and under-*  
13 *stand the processing purpose for which*  
14 *consent is sought and the covered data*  
15 *to be collected, processed, or transferred*  
16 *by the covered entity for such proc-*  
17 *essing purpose.*

18                   (iii) *The request clearly explains the*  
19 *individual's applicable rights related to con-*  
20 *sent.*

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

24                   (v) *The request is made available to the*  
25 *individual in each covered language in*

1           *which the covered entity provides a product*  
2           *or service for which authorization is sought.*

3           *(vi) The option to refuse consent shall*  
4           *be at least as prominent as the option to ac-*  
5           *cept, and the option to refuse consent shall*  
6           *take the same number of steps or fewer as*  
7           *the option to accept.*

8           *(vii) Processing or transferring any*  
9           *covered data collected pursuant to affirma-*  
10          *tive express consent for a different proc-*  
11          *essing purpose than that for which affirma-*  
12          *tive express consent was obtained shall re-*  
13          *quire affirmative express consent for the*  
14          *subsequent processing purpose.*

15          *(C) EXPRESS CONSENT REQUIRED.—A cov-*  
16          *ered entity may not infer that an individual has*  
17          *provided affirmative express consent to an act or*  
18          *practice from the inaction of the individual or*  
19          *the individual's continued use of a service or*  
20          *product provided by the covered entity.*

21          *(D) PRETEXTUAL CONSENT PROHIBITED.—*  
22          *A covered entity may not obtain or attempt to*  
23          *obtain the affirmative express consent of an indi-*  
24          *vidual through—*

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

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

11                   (2) *AUTHENTICATION.—The term “authentic-*  
12                   *ation” means the process of verifying an individual or*  
13                   *entity for security purposes.*

14                   (3) *BIOMETRIC INFORMATION.—*

15                   (A) *IN GENERAL.—The term “biometric in-*  
16                   *formation” means any covered data generated*  
17                   *from the technological processing of an individ-*  
18                   *ual’s unique biological, physical, or physiological*  
19                   *characteristics that is linked or reasonably*  
20                   *linkable to an individual, including—*

21                   (i) *fingerprints;*

22                   (ii) *voice prints;*

23                   (iii) *iris or retina scans;*

24                   (iv) *facial or hand mapping, geometry,*  
25                   *or templates; or*

1                   (v) gait or personally identifying phys-  
2                   ical movements.

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

5                   (i) a digital or physical photograph;

6                   (ii) an audio or video recording; or

7                   (iii) data generated from a digital or  
8                   physical photograph, or an audio or video  
9                   recording, that cannot be used to identify  
10                  an individual.

11                 (4) *COLLECT; COLLECTION.*—The terms “collect”  
12                 and “collection” mean buying, renting, gathering, ob-  
13                 taining, receiving, accessing, or otherwise acquiring  
14                 covered data by any means.

15                 (5) *COMMISSION.*—The term “Commission”  
16                 means the Federal Trade Commission.

17                 (6) *CONTROL.*—The term “control” means, with  
18                 respect to an entity—

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

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



1                   (C) *the power to exercise a controlling influ-*  
2                   *ence over the management of the entity.*

3                   (7) *COVERED ALGORITHM.—The term “covered*  
4                   *algorithm” means a computational process that uses*  
5                   *machine learning, natural language processing, arti-*  
6                   *ficial intelligence techniques, or other computational*  
7                   *processing techniques of similar or greater complexity*  
8                   *and that makes a decision or facilitates human deci-*  
9                   *sion-making with respect to covered data, including*  
10                   *to determine the provision of products or services or*  
11                   *to rank, order, promote, recommend, amplify, or*  
12                   *similarly determine the delivery or display of infor-*  
13                   *mation to an individual.*

14                   (8) *COVERED DATA.—*

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

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

24                                   (i) *de-identified data;*

25                                   (ii) *employee data;*

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

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

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

- 19                   (ii) information processed by an em-  
20 ployer relating to an employee who is act-  
21 ing in a professional capacity for the em-  
22 ployer, provided that such information is  
23 collected, processed, or transferred solely for  
24 purposes related to such employee’s profes-  
25 sional activities on behalf of the employer;

1                   (iii) the business contact information  
2 of an employee, including the employee's  
3 name, position or title, business telephone  
4 number, business address, or business email  
5 address that is provided to an employer by  
6 an employee who is acting in a professional  
7 capacity, if such information is collected,  
8 processed, or transferred solely for purposes  
9 related to such employee's professional ac-  
10 tivities on behalf of the employer;

11                   (iv) emergency contact information col-  
12 lected by an employer that relates to an em-  
13 ployee of that employer, if such information  
14 is collected, processed, or transferred solely  
15 for the purpose of having an emergency con-  
16 tact on file for the employee and for proc-  
17 essing or transferring such information in  
18 case of an emergency; or

19                   (v) information relating to an em-  
20 ployee (or a spouse, dependent, other covered  
21 family member, or beneficiary of such em-  
22 ployee) that is necessary for the employer to  
23 collect, process, or transfer solely for the  
24 purpose of administering benefits to which  
25 such employee (or spouse, dependent, other

1           *covered family member, or beneficiary of*  
2           *such employee) is entitled on the basis of the*  
3           *employee’s position with that employer.*

4           (9) *COVERED ENTITY.—*

5           (A) *IN GENERAL.—The term “covered enti-*  
6           *ty”—*

7                   (i) *means any entity or any person,*  
8                   *other than an individual acting in a non-*  
9                   *commercial context, that alone or jointly*  
10                  *with others determines the purposes and*  
11                  *means of collecting, processing, or transfer-*  
12                  *ring covered data and—*

13                           (I) *is subject to the Federal Trade*  
14                           *Commission Act (15 U.S.C. 41 et seq.);*

15                           (II) *is a common carrier subject*  
16                           *to the Communications Act of 1934 (47*  
17                           *U.S.C. 151 et seq.) and all Acts*  
18                           *amendatory thereof and supplementary*  
19                           *thereto; or*

20                           (III) *is an organization not orga-*  
21                           *nized to carry on business for its own*  
22                           *profit or that of its members; and*

23                           (ii) *includes any entity or person that*  
24                           *controls, is controlled by, or is under com-*  
25                           *mon control with the covered entity.*

1                   (B) *EXCLUSIONS.*—*The term “covered enti-*  
2                   *ty” does not include—*

3                   (i) *a Federal, State, Tribal, territorial,*  
4                   *or local government entity such as a body,*  
5                   *authority, board, bureau, commission, dis-*  
6                   *trict, agency, or political subdivision of the*  
7                   *Federal Government or a State, Tribal, ter-*  
8                   *ritorial, or local government;*

9                   (ii) *a person or an entity that is col-*  
10                   *lecting, processing, or transferring covered*  
11                   *data on behalf of a Federal, State, Tribal,*  
12                   *territorial, or local government entity, in so*  
13                   *far as such person or entity is acting as a*  
14                   *service provider to the government entity; or*

15                   (iii) *an entity that serves as a congres-*  
16                   *sionally designated nonprofit, national re-*  
17                   *source center, and clearinghouse to provide*  
18                   *assistance to victims, families, child-serving*  
19                   *professionals, and the general public on*  
20                   *missing and exploited children issues.*

21                   (C) *NON-APPLICATION TO SERVICE PRO-*  
22                   *VIDERS.*—*An entity shall not be considered to be*  
23                   *a covered entity for purposes of this Act in so far*  
24                   *as the entity is acting as a service provider (as*  
25                   *defined in paragraph (29)).*

1           (10) *COVERED LANGUAGE.*—*The term “covered*  
2 *language” means the ten languages with the most*  
3 *users in the United States, according to the most re-*  
4 *cent United States Census.*

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

7           (12) *DE-IDENTIFIED DATA.*—*The term “de-iden-*  
8 *tified data” means information that does not identify*  
9 *and is not linked or reasonably linkable to a distinct*  
10 *individual or a device, regardless of whether the infor-*  
11 *mation is aggregated, and if the covered entity or*  
12 *service provider—*

13                 (A) *takes reasonable technical measures to*  
14 *ensure that the information cannot, at any*  
15 *point, be used to re-identify any individual or*  
16 *device that identifies or is linked or reasonably*  
17 *linkable to an individual;*

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

20                         (i) *to process and transfer the informa-*  
21 *tion solely in a de-identified form without*  
22 *any reasonable means for re-identification;*  
23 *and*

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

1                   that identifies or is linked or reasonably  
2                   linkable to an individual; and

3                   (C) contractually obligates any person or  
4                   entity that receives the information from the cov-  
5                   ered entity or service provider—

6                   (i) to comply with all of the provisions  
7                   of this paragraph with respect to the infor-  
8                   mation; and

9                   (ii) to require that such contractual ob-  
10                  ligations be included contractually in all  
11                  subsequent instances for which the data  
12                  may be received.

13                  (13) *DERIVED DATA.*—The term “derived data”  
14                  means covered data that is created by the derivation  
15                  of information, data, assumptions, correlations, infer-  
16                  ences, predictions, or conclusions from facts, evidence,  
17                  or another source of information or data about an in-  
18                  dividual or an individual’s device.

19                  (14) *DEVICE.*—The term “device” means any  
20                  electronic equipment capable of collecting, processing,  
21                  or transferring covered data that is used by one or  
22                  more individuals.

23                  (15) *EMPLOYEE.*—The term “employee” means  
24                  an individual who is an employee, director, officer,  
25                  staff member individual working as an independent

1        *contractor that is not a service provider, trainee, vol-*  
2        *unteer, or intern of an employer, regardless of whether*  
3        *such individual is paid, unpaid, or employed on a*  
4        *temporary basis.*

5            (16) *EXECUTIVE AGENCY.*—*The “Executive agen-*  
6        *cy” has the meaning given such term in section 105*  
7        *of title 5, United States Code.*

8            (17) *FIRST PARTY ADVERTISING OR MAR-*  
9        *KETING.*—*The term “first party advertising or mar-*  
10       *keting” means advertising or marketing conducted by*  
11       *a first party either through direct communications*  
12       *with a user such as direct mail, email, or text mes-*  
13       *sage communications, or advertising or marketing*  
14       *conducted entirely within the first-party context, such*  
15       *as in a physical location operated by the first party,*  
16       *or on a web site or app operated by the first party.*

17            (18) *GENETIC INFORMATION.*—*The term “genetic*  
18       *information” means any covered data, regardless of*  
19       *its format, that concerns an individual’s genetic char-*  
20       *acteristics, including—*

21            (A) *raw sequence data that results from the*  
22        *sequencing of the complete, or a portion of the,*  
23        *extracted deoxyribonucleic acid (DNA) of an in-*  
24        *dividual; or*



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

4           (19) *INDIVIDUAL.—The term “individual” means*  
5           *a natural person residing in the United States.*

6           (20) *KNOWLEDGE.—*

7           (A) *IN GENERAL.—The term “knowledge”*  
8           *means—*

9                   (i) *with respect to a covered entity that*  
10                  *is a covered high-impact social media com-*  
11                  *pany, the entity knew or should have known*  
12                  *the individual was a covered minor;*

13                   (ii) *with respect to a covered entity or*  
14                  *service provider that is a large data holder,*  
15                  *and otherwise is not a covered high-impact*  
16                  *social media company, that the covered en-*  
17                  *tity knew or acted in willful disregard of*  
18                  *the fact that the individual was a covered*  
19                  *minor; and*

20                   (iii) *with respect to a covered entity or*  
21                  *service provider that does not meet the re-*  
22                  *quirements of clause (i) or (ii), actual*  
23                  *knowledge.*

24           (B) *COVERED HIGH-IMPACT SOCIAL MEDIA*  
25           *COMPANY.—For purposes of this paragraph, the*

1           *term “covered high-impact social media com-*  
2           *pany” means a covered entity that provides any*  
3           *internet-accessible platform where—*

4                     *(i) such covered entity generates*  
5                     *\$3,000,000,000 or more in annual revenue;*

6                     *(ii) such platform has 300,000,000 or*  
7                     *more monthly active users for not fewer*  
8                     *than 3 of the preceding 12 months on the*  
9                     *online product or service of such covered en-*  
10                    *tity; and*

11                    *(iii) such platform constitutes an on-*  
12                    *line product or service that is primarily*  
13                    *used by users to access or share, user-gen-*  
14                    *erated content.*

15            (21) *LARGE DATA HOLDER.—*

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

19                             *(i) had annual gross revenues of*  
20                             *\$250,000,000 or more; and*

21                             *(ii) collected, processed, or trans-*  
22                             *ferred—*

23                                     (I) *the covered data of more than*  
24                                     *5,000,000 individuals or devices that*  
25                                     *identify or are linked or reasonably*

1                    *linkable to 1 or more individuals, ex-*  
2                    *cluding covered data collected and*  
3                    *processed solely for the purpose of ini-*  
4                    *tiating, rendering, billing for, final-*  
5                    *izing, completing, or otherwise col-*  
6                    *lecting payment for a requested prod-*  
7                    *uct or service; and*

8                    *(II) the sensitive covered data of*  
9                    *more than 200,000 individuals or de-*  
10                   *vices that identify or are linked or rea-*  
11                   *sonably linkable to 1 or more individ-*  
12                   *uals.*

13                   *(B) EXCLUSIONS.—The term “large data*  
14                   *holder” does not include any instance in which*  
15                   *the covered entity or service provider would qual-*  
16                   *ify as a large data holder solely on the basis of*  
17                   *collecting or processing—*

18                   *(i) personal email addresses;*

19                   *(ii) personal telephone numbers; or*

20                   *(iii) log-in information of an indi-*  
21                   *vidual or device to allow the individual or*  
22                   *device to log in to an account administered*  
23                   *by the covered entity or service provider.*

24                   *(C) REVENUE.—For purposes of deter-*  
25                   *mining whether any covered entity or service*

1            *provider is a large data holder, the term “rev-*  
2            *enue”, with respect to any covered entity or serv-*  
3            *ice provider that is not organized to carry on*  
4            *business for its own profit or that of its mem-*  
5            *bers—*

6                    *(i) means the gross receipts the covered*  
7                    *entity or service provider received, in what-*  
8                    *ever form, from all sources, without sub-*  
9                    *tracting any costs or expenses; and*

10                   *(ii) includes contributions, gifts,*  
11                   *grants, dues or other assessments, income*  
12                   *from investments, and proceeds from the*  
13                   *sale of real or personal property.*

14            *(22) MARKET RESEARCH.—The term “market re-*  
15            *search” means the collection, processing, or transfer of*  
16            *covered data as reasonably necessary and propor-*  
17            *tionate to investigate the market for or marketing of*  
18            *products, services, or ideas, where the covered data is*  
19            *not—*

20                    *(A) integrated into any product or service;*

21                    *(B) otherwise used to contact any indi-*  
22                    *vidual or individual’s device; or*

23                    *(C) used to advertise or market to any indi-*  
24                    *vidual or individual’s device.*

1           (23) *MATERIAL.*—*The term “material” means,*  
2           *with respect to an act, practice, or representation of*  
3           *a covered entity (including a representation made by*  
4           *the covered entity in a privacy policy or similar dis-*  
5           *closure to individuals) involving the collection, proc-*  
6           *essing, or transfer of covered data, that such act,*  
7           *practice, or representation is likely to affect a reason-*  
8           *able individual’s decision or conduct regarding a*  
9           *product or service.*

10           (24) *PRECISE GEOLOCATION INFORMATION.*—

11           (A) *IN GENERAL.*—*The term “precise*  
12           *geolocation information” means information that*  
13           *is derived from a device or technology that re-*  
14           *veals the past or present physical location of an*  
15           *individual or device that identifies or is linked*  
16           *or reasonably linkable to 1 or more individuals,*  
17           *with sufficient precision to identify street level*  
18           *location information of an individual or device*  
19           *or the location of an individual or device within*  
20           *a range of 1,850 feet or less.*

21           (B) *EXCLUSION.*—*The term “precise*  
22           *geolocation information” does not include*  
23           *geolocation information identifiable or derived*  
24           *solely from the visual content of a legally ob-*

1           *tained image, including the location of the device*  
2           *that captured such image.*

3           (25) *PROCESS.—The term “process” means to*  
4           *conduct or direct any operation or set of operations*  
5           *performed on covered data, including analyzing, orga-*  
6           *nizing, structuring, retaining, storing, using, or oth-*  
7           *erwise handling covered data.*

8           (26) *PROCESSING PURPOSE.—The term “proc-*  
9           *essing purpose” means a reason for which a covered*  
10          *entity or service provider collects, processes, or trans-*  
11          *fers covered data that is specific and granular enough*  
12          *for a reasonable individual to understand the mate-*  
13          *rial facts of how and why the covered entity or service*  
14          *provider collects, processes, or transfers the covered*  
15          *data.*

16          (27) *PUBLICLY AVAILABLE INFORMATION.—*

17                (A) *IN GENERAL.—The term “publicly*  
18                *available information” means any information*  
19                *that a covered entity or service provider has a*  
20                *reasonable basis to believe has been lawfully*  
21                *made available to the general public from—*

22                        (i) *Federal, State, or local government*  
23                        *records, if the covered entity collects, proc-*  
24                        *esses, and transfers such information in ac-*  
25                        *cordance with any restrictions or terms of*

1                    *use placed on the information by the rel-*  
2                    *evant government entity;*

3                    *(ii) widely distributed media;*

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

9                    *(iv) a disclosure that has been made to*  
10                   *the general public as required by Federal,*  
11                   *State, or local law; or*

12                   *(v) the visual observation of the phys-*  
13                   *ical presence of an individual or a device in*  
14                   *a public place, not including data collected*  
15                   *by a device in the individual's possession.*

16                   *(B) CLARIFICATIONS; LIMITATIONS.—*

17                   *(i) AVAILABLE TO ALL MEMBERS OF*  
18                   *THE PUBLIC.—For purposes of this para-*  
19                   *graph, information from a website or online*  
20                   *service is not available to all members of the*  
21                   *public if the individual who made the infor-*  
22                   *mation available via the website or online*  
23                   *service has restricted the information to a*  
24                   *specific audience.*

1                   (ii) *OTHER LIMITATIONS.*—*The term*  
2                   “*publicly available information*” *does not*  
3                   *include—*

4                   (I) *any obscene visual depiction*  
5                   *(as defined in section 1460 of title 18,*  
6                   *United States Code);*

7                   (II) *any inference made exclu-*  
8                   *sively from multiple independent*  
9                   *sources of publicly available informa-*  
10                   *tion that reveals sensitive covered data*  
11                   *with respect to an individual;*

12                   (III) *biometric information;*

13                   (IV) *publicly available informa-*  
14                   *tion that has been combined with cov-*  
15                   *ered data;*

16                   (V) *genetic information, unless*  
17                   *otherwise made available by the indi-*  
18                   *vidual to whom the information per-*  
19                   *tains as described in clause (ii) or (iii)*  
20                   *of subparagraph (A); or*

21                   (VI) *intimate images known to be*  
22                   *nonconsensual.*

23                   (28) *SENSITIVE COVERED DATA.*—



1                   (A) *IN GENERAL.*—*The term “sensitive cov-*  
2 *ered data” means the following types of covered*  
3 *data:*

4                   (i) *A government-issued identifier,*  
5 *such as a Social Security number, passport*  
6 *number, or driver’s license number, that is*  
7 *not required by law to be displayed in pub-*  
8 *lic.*

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

14                   (iii) *A financial account number, debit*  
15 *card number, credit card number, or infor-*  
16 *mation that describes or reveals the income*  
17 *level or bank account balances of an indi-*  
18 *vidual, except that the last four digits of a*  
19 *debit or credit card number shall not be*  
20 *deemed sensitive covered data.*

21                   (iv) *Biometric information.*

22                   (v) *Genetic information.*

23                   (vi) *Precise geolocation information.*

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

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

21                   *(viii) Account or device log-in creden-*  
22                   *tials, or security or access codes for an ac-*  
23                   *count or device.*

24                   *(ix) Information identifying the sexual*  
25                   *behavior of an individual in a manner in-*

1                   *consistent with the individual's reasonable*  
2                   *expectation regarding the collection, proc-*  
3                   *essing, or transfer of such information.*

4                   *(x) Calendar information, address book*  
5                   *information, phone or text logs, photos,*  
6                   *audio recordings, or videos, maintained for*  
7                   *private use by an individual, regardless of*  
8                   *whether such information is stored on the*  
9                   *individual's device or is accessible from that*  
10                  *device and is backed up in a separate loca-*  
11                  *tion. Such information is not sensitive for*  
12                  *purposes of this paragraph if such informa-*  
13                  *tion is sent from or to a device provided by*  
14                  *an employer to an employee insofar as such*  
15                  *employer provides conspicuous notice that it*  
16                  *may access such information.*

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

21                  *(xii) Information revealing the video*  
22                  *content requested or selected by an indi-*  
23                  *vidual collected by a covered entity that is*  
24                  *not a provider of a service described in sec-*  
25                  *tion 102(4). This clause does not include*

1 covered data used solely for transfers for  
2 independent video measurement.

3 (xiii) Information about an individual  
4 when the covered entity or service provider  
5 has knowledge that the individual is a cov-  
6 ered minor.

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

9 (xv) Information identifying an indi-  
10 vidual's online activities over time and  
11 across third party websites or online serv-  
12 ices.

13 (xvi) Any other covered data collected,  
14 processed, or transferred for the purpose of  
15 identifying the types of covered data listed  
16 in clauses (i) through (xv).

17 (B) RULEMAKING.—The Commission may  
18 commence a rulemaking pursuant to section 553  
19 of title 5, United States Code, to include in the  
20 definition of “sensitive covered data” any other  
21 type of covered data that may require a similar  
22 level of protection as the types of covered data  
23 listed in clauses (i) through (xvi) of subpara-  
24 graph (A) as a result of any new method of col-  
25 lecting, processing, or transferring covered data.

1           (29) *SERVICE PROVIDER.*—

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

4                           (i) *collects, processes, or transfers cov-*  
5 *ered data on behalf of, and at the direction*  
6 *of, a covered entity or a Federal, State,*  
7 *Tribal, territorial, or local government enti-*  
8 *ty; and*

9                           (ii) *receives covered data from or on*  
10 *behalf of a covered entity or a Federal,*  
11 *State, Tribal, territorial, or local govern-*  
12 *ment entity.*

13                   (B) *TREATMENT WITH RESPECT TO SERV-*  
14 *ICE PROVIDER DATA.*—*A service provider that re-*  
15 *ceives service provider data from another service*  
16 *provider as permitted under this Act shall be*  
17 *treated as a service provider under this Act with*  
18 *respect to such data.*

19           (30) *SERVICE PROVIDER DATA.*—*The term “serv-*  
20 *ice provider data” means covered data that is col-*  
21 *lected or processed by or has been transferred to a*  
22 *service provider by or on behalf of a covered entity,*  
23 *a Federal, State, Tribal, territorial, or local govern-*  
24 *ment entity, or another service provider for the pur-*  
25 *pose of allowing the service provider to whom such*

1        *covered data is transferred to perform a service or*  
2        *function on behalf of, and at the direction of, such*  
3        *covered entity or Federal, State, Tribal, territorial, or*  
4        *local government entity.*

5            (31) *STATE.*—*The term “State” means any of*  
6        *the 50 States, the District of Columbia, the Common-*  
7        *wealth of Puerto Rico, the Virgin Islands of the*  
8        *United States, Guam, American Samoa, or the Com-*  
9        *monwealth of the Northern Mariana Islands.*

10           (32) *STATE PRIVACY AUTHORITY.*—*The term*  
11        *“State privacy authority” means—*

12                (A) *the chief consumer protection officer of*  
13        *a State; or*

14                (B) *a State consumer protection agency*  
15        *with expertise in data protection, including the*  
16        *California Privacy Protection Agency.*

17           (33) *SUBSTANTIAL PRIVACY RISK.*—*The term*  
18        *“substantial privacy risk” means the collection, proc-*  
19        *essing, or transfer of covered data in a manner that*  
20        *may result in any reasonably foreseeable substantial*  
21        *physical injury, economic injury, highly offensive in-*  
22        *trusion into the privacy expectations of a reasonable*  
23        *individual under the circumstances, or discrimina-*  
24        *tion on the basis of race, color, religion, national ori-*  
25        *gin, sex, or disability.*

1           (34) *TARGETED ADVERTISING.*—The term “tar-  
2           geted advertising”—

3                   (A) means presenting to an individual or  
4                   device identified by a unique identifier, or  
5                   groups of individuals or devices identified by  
6                   unique identifiers, an online advertisement that  
7                   is selected based on known or predicted pref-  
8                   erences, characteristics, or interests associated  
9                   with the individual or a device identified by a  
10                  unique identifier; and

11                  (B) does not include—

12                   (i) advertising or marketing to an in-  
13                   dividual or an individual’s device in re-  
14                   sponse to the individual’s specific request  
15                   for information or feedback;

16                   (ii) contextual advertising, which is  
17                   when an advertisement is displayed based  
18                   on the content in which the advertisement  
19                   appears and does not vary based on who is  
20                   viewing the advertisement; or

21                   (iii) processing covered data solely for  
22                   measuring or reporting advertising or con-  
23                   tent, performance, reach, or frequency, in-  
24                   cluding independent measurement.

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

1           (A) means any person or entity, including  
2 a covered entity, that—

3           (i) collects, processes, or transfers cov-  
4 ered data that the person or entity did not  
5 collect directly from the individual linked or  
6 linkable to such covered data; and

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

9           (B) does not include a person or entity that  
10 collects covered data from another entity if the 2  
11 entities are related by common ownership or cor-  
12 porate control, but only if a reasonable con-  
13 sumer's reasonable expectation would be that  
14 such entities share information.

15 (36) *THIRD-PARTY COLLECTING ENTITY.*—

16           (A) *IN GENERAL.*—The term “third-party  
17 collecting entity”—

18           (i) means a covered entity whose prin-  
19 cipal source of revenue is derived from proc-  
20 essing or transferring covered data that the  
21 covered entity did not collect directly from  
22 the individuals linked or linkable to the cov-  
23 ered data; and

24           (ii) does not include a covered entity  
25 insofar as such entity processes employee



1           *data collected by and received from a third*  
2           *party concerning any individual who is an*  
3           *employee of the third party for the sole pur-*  
4           *pose of such third party providing benefits*  
5           *to the employee.*

6           *(B) PRINCIPAL SOURCE OF REVENUE DE-*  
7           *FINED.—For purposes of this paragraph, the*  
8           *term “principal source of revenue” means, for*  
9           *the prior 12-month period, either—*

10                   *(i) more than 50 percent of all revenue*  
11                   *of the covered entity; or*

12                   *(ii) obtaining revenue from processing*  
13                   *or transferring the covered data of more*  
14                   *than 5,000,000 individuals that the covered*  
15                   *entity did not collect directly from the indi-*  
16                   *viduals linked or linkable to the covered*  
17                   *data.*

18           *(C) NON-APPLICATION TO SERVICE PRO-*  
19           *VIDERS.—An entity may not be considered to be*  
20           *a third-party collecting entity for purposes of*  
21           *this Act if the entity is acting as a service pro-*  
22           *vider.*

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

1           (38) *TRANSFER*.—The term “transfer” means to  
2           disclose, release, disseminate, make available, license,  
3           rent, or share covered data orally, in writing, elec-  
4           tronically, or by any other means.

5           (39) *UNIQUE PERSISTENT IDENTIFIER*.—The  
6           term “unique identifier”—

7           (A) means an identifier to the extent that  
8           such identifier is reasonably linkable to an indi-  
9           vidual or device that identifies or is linked or  
10          reasonably linkable to 1 or more individuals, in-  
11          cluding a device identifier, Internet Protocol ad-  
12          dress, cookie, beacon, pixel tag, mobile ad identi-  
13          fier, or similar technology, customer number,  
14          unique pseudonym, user alias, telephone number,  
15          or other form of persistent or probabilistic iden-  
16          tifier that is linked or reasonably linkable to an  
17          individual or device; and

18          (B) does not include an identifier assigned  
19          by a covered entity for the specific purpose of  
20          giving effect to an individual’s exercise of affirm-  
21          ative express consent or opt-outs of the collection,  
22          processing, and transfer of covered data pursu-  
23          ant to section 204 or otherwise limiting the col-  
24          lection, processing, or transfer of such informa-  
25          tion.

1           (40) *WIDELY DISTRIBUTED MEDIA*.—The term  
2           “widely distributed media” means information that  
3           is available to the general public, including informa-  
4           tion from a telephone book or online directory, a tele-  
5           vision, internet, or radio program, the news media, or  
6           an internet site that is available to the general public  
7           on an unrestricted basis, but does not include an ob-  
8           scene visual depiction (as defined in section 1460 of  
9           title 18, United States Code).

## 10           **TITLE I—DUTY OF LOYALTY**

### 11           **SEC. 101. DATA MINIMIZATION.**

12           (a) *IN GENERAL*.—A covered entity may not collect,  
13           process, or transfer covered data unless the collection, proc-  
14           essing, or transfer is limited to what is reasonably necessary  
15           and proportionate to—

16                   (1) provide or maintain a specific product or  
17                   service requested by the individual to whom the data  
18                   pertains; or

19                   (2) effect a purpose permitted under subsection  
20                   (b).

21           (b) *PERMISSIBLE PURPOSES*.—A covered entity may  
22           collect, process, or transfer covered data for any of the fol-  
23           lowing purposes if the collection, processing, or transfer is  
24           limited to what is reasonably necessary and proportionate  
25           to such purpose:

1           (1) *To initiate, manage, or complete a trans-*  
2 *action or fulfill an order for specific products or serv-*  
3 *ices requested by an individual, including any associ-*  
4 *ated routine administrative, operational, and ac-*  
5 *count-servicing activity such as billing, shipping, de-*  
6 *livery, storage, and accounting.*

7           (2) *With respect to covered data previously col-*  
8 *lected in accordance with this Act, notwithstanding*  
9 *this exception—*

10                   (A) *to process such data as necessary to per-*  
11 *form system maintenance or diagnostics;*

12                   (B) *to develop, maintain, repair, or enhance*  
13 *a product or service for which such data was col-*  
14 *lected;*

15                   (C) *to conduct internal research or ana-*  
16 *lytics to improve a product or service for which*  
17 *such data was collected;*

18                   (D) *to perform inventory management or*  
19 *reasonable network management;*

20                   (E) *to protect against spam; or*

21                   (F) *to debug or repair errors that impair*  
22 *the functionality of a service or product for*  
23 *which such data was collected.*

24           (3) *To authenticate users of a product or service.*

25           (4) *To fulfill a product or service warranty.*

1           (5) *To prevent, detect, protect against, or re-*  
2           *pond to a security incident. For purposes of this*  
3           *paragraph, security is defined as network security*  
4           *and physical security and life safety, including an*  
5           *intrusion or trespass, medical alerts, fire alarms, and*  
6           *access control security.*

7           (6) *To prevent, detect, protect against, or re-*  
8           *pond to fraud, harassment, or illegal activity. For*  
9           *purposes of this paragraph, the term “illegal activity”*  
10          *means a violation of a Federal, State, or local law*  
11          *punishable as a felony or misdemeanor that can di-*  
12          *rectly harm.*

13          (7) *To comply with a legal obligation imposed*  
14          *by Federal, Tribal, local, or State law, or to inves-*  
15          *tigate, establish, prepare for, exercise, or defend legal*  
16          *claims involving the covered entity or service pro-*  
17          *vider.*

18          (8) *To prevent an individual, or group of indi-*  
19          *viduals, from suffering harm where the covered entity*  
20          *or service provider believes in good faith that the in-*  
21          *dividual, or group of individuals, is at risk of death,*  
22          *serious physical injury, or other serious health risk.*

23          (9) *To effectuate a product recall pursuant to*  
24          *Federal or State law.*

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

4                     *(i) is in the public interest; and*

5                     *(ii) adheres to all relevant laws and regula-*  
6           *tions governing such research, including regula-*  
7           *tions for the protection of human subjects, or is*  
8           *excluded from criteria of the institutional review*  
9           *board.*

10           (B) *Not later than 18 months after the date of*  
11           *enactment of this Act, the Commission should issue*  
12           *guidelines to help covered entities ensure the privacy*  
13           *of affected users and the security of covered data, par-*  
14           *ticularly as data is being transferred to and stored by*  
15           *researchers. Such guidelines should consider risks as*  
16           *they pertain to projects using covered data with spe-*  
17           *cial considerations for projects that are exempt under*  
18           *part 46 of title 45, Code of Federal Regulations (or*  
19           *any successor regulation) or are excluded from the*  
20           *criteria for institutional review board review.*

21           (11) *To deliver a communication that is not an*  
22           *advertisement to an individual, if the communication*  
23           *is reasonably anticipated by the individual within the*  
24           *context of the individual's interactions with the cov-*  
25           *ered entity.*

1           (12) *To deliver a communication at the direction*  
2 *of an individual between such individual and one or*  
3 *more individuals or entities.*

4           (13) *To transfer assets to a third party in the*  
5 *context of a merger, acquisition, bankruptcy, or simi-*  
6 *lar transaction when the third party assumes control,*  
7 *in whole or in part, of the covered entity's assets, only*  
8 *if the covered entity, in a reasonable time prior to*  
9 *such transfer, provides each affected individual*  
10 *with—*

11           (A) *a notice describing such transfer, in-*  
12 *cluding the name of the entity or entities receiv-*  
13 *ing the individual's covered data and their pri-*  
14 *vacancy policies as described in section 202; and*

15           (B) *a reasonable opportunity to withdraw*  
16 *any previously given consents in accordance*  
17 *with the requirements of affirmative express con-*  
18 *sent under this Act related to the individual's*  
19 *covered data and a reasonable opportunity to re-*  
20 *quest the deletion of the individual's covered*  
21 *data, as described in section 203.*

22           (14) *To ensure the data security and integrity of*  
23 *covered data, as described in section 208.*

24           (15) *With respect to covered data previously col-*  
25 *lected in accordance with this Act, a service provider*

1        *acting at the direction of a government entity, or a*  
2        *service provided to a government entity by a covered*  
3        *entity, and only insofar as authorized by statute, to*  
4        *prevent, detect, protect against or respond to a public*  
5        *safety incident, including trespass, natural disaster,*  
6        *or national security incident. This paragraph does*  
7        *not permit, however, the transfer of covered data for*  
8        *payment or other valuable consideration to a govern-*  
9        *ment entity.*

10            *(16) With respect to covered data collected in ac-*  
11            *cordance with this Act, notwithstanding this excep-*  
12            *tion, to process such data as necessary to provide first*  
13            *party advertising or marketing of products or services*  
14            *provided by the covered entity for individuals who are*  
15            *not-covered minors.*

16            *(17) With respect to covered data previously col-*  
17            *lected in accordance with this Act, notwithstanding*  
18            *this exception and provided such collection, proc-*  
19            *essing, and transferring otherwise complies with the*  
20            *requirements of this Act, including section 204(c), to*  
21            *provide targeted advertising.*

22            *(c) GUIDANCE.—The Commission shall issue guidance*  
23            *regarding what is reasonably necessary and proportionate*  
24            *to comply with this section. Such guidance shall take into*  
25            *consideration—*



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

7           (2) *the sensitivity of covered data collected, proc-*  
8           *essed, or transferred by the covered entity;*

9           (3) *the volume of covered data collected, proc-*  
10          *essed, or transferred by the covered entity; and*

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

14          (d) *DECEPTIVE MARKETING OF A PRODUCT OR SERV-*  
15          *ICE.—A covered entity or service provider may not engage*  
16          *in deceptive advertising or marketing with respect to a*  
17          *product or service offered to an individual.*

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

21          **SEC. 102. LOYALTY DUTIES.**

22          *Notwithstanding section 101 and unless an exception*  
23          *applies, with respect to covered data, a covered entity or*  
24          *service provider may not—*

1           (1) *collect, process, or transfer a Social Security*  
2           *number, except when necessary to facilitate an exten-*  
3           *sion of credit, authentication, fraud and identity*  
4           *fraud detection and prevention, the payment or collec-*  
5           *tion of taxes, the enforcement of a contract between*  
6           *parties, or the prevention, investigation, or prosecu-*  
7           *tion of fraud or illegal activity, or as otherwise re-*  
8           *quired by Federal, State, or local law;*

9           (2) *collect or process sensitive covered data, ex-*  
10          *cept where such collection or processing is strictly nec-*  
11          *essary to provide or maintain a specific product or*  
12          *service requested by the individual to whom the cov-*  
13          *ered data pertains, or is strictly necessary to effect a*  
14          *purpose enumerated in paragraphs (1) through (12)*  
15          *and (14) through (15) of section 101(b);*

16          (3) *transfer an individual's sensitive covered*  
17          *data to a third party, unless—*

18                 (A) *the transfer is made pursuant to the af-*  
19                 *firmative express consent of the individual;*

20                 (B) *the transfer is necessary to comply with*  
21                 *a legal obligation imposed by Federal, State,*  
22                 *Tribal, or local law, or to establish, exercise, or*  
23                 *defend legal claims;*

24                 (C) *the transfer is necessary to prevent an*  
25                 *individual from imminent injury where the cov-*

1            *ered entity believes in good faith that the indi-*  
2            *vidual is at risk of death, serious physical in-*  
3            *jury, or serious health risk;*

4            *(D) with respect to covered data collected in*  
5            *accordance with this Act, notwithstanding this*  
6            *exception, a service provider acting at the direc-*  
7            *tion of a government entity, or a service pro-*  
8            *vided to a government entity by a covered entity,*  
9            *and only insofar as authorized by statute, the*  
10           *transfer is necessary to prevent, detect, protect*  
11           *against or respond to a public safety incident in-*  
12           *cluding trespass, natural disaster, or national se-*  
13           *curity incident. This paragraph does not permit,*  
14           *however, the transfer of covered data for payment*  
15           *or other valuable consideration to a government*  
16           *entity;*

17           *(E) in the case of the transfer of a pass-*  
18           *word, the transfer is necessary to use a des-*  
19           *ignated password manager or is to a covered en-*  
20           *tity for the exclusive purpose of identifying pass-*  
21           *words that are being re-used across sites or ac-*  
22           *counts;*

23           *(F) in the case of the transfer of genetic in-*  
24           *formation, the transfer is necessary to perform a*  
25           *medical diagnosis or medical treatment specifi-*

1 *cally requested by an individual, or to conduct*  
2 *medical research in accordance with conditions*  
3 *of section 101(b)(10); or*

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

6 *(4) in the case of a provider of broadcast tele-*  
7 *vision service, cable service, satellite service, stream-*  
8 *ing media service, or other video programming service*  
9 *described in section 713(h)(2) of the Communications*  
10 *Act of 1934 (47 U.S.C. 613(h)(2)), transfer to an un-*  
11 *affiliated third party covered data that reveals the*  
12 *video content or services requested or selected by an*  
13 *individual from such service, except with the affirma-*  
14 *tive express consent of the individual or pursuant to*  
15 *one of the permissible purposes enumerated in para-*  
16 *graphs (1) through (15) of section 101(b).*

17 **SEC. 103. PRIVACY BY DESIGN.**

18 *(a) POLICIES, PRACTICES, AND PROCEDURES.—A cov-*  
19 *ered entity and a service provider shall establish, imple-*  
20 *ment, and maintain reasonable policies, practices, and pro-*  
21 *cedures that reflect the role of the covered entity or service*  
22 *provider in the collection, processing, and transferring of*  
23 *covered data and that—*

1           (1) *consider applicable Federal laws, rules, or*  
2 *regulations related to covered data the covered entity*  
3 *or service provider collects, processes, or transfers;*

4           (2) *identify, assess, and mitigate privacy risks*  
5 *related to covered minors (including, if applicable,*  
6 *with respect to a covered entity that is not an entity*  
7 *meeting the requirements of section 209, in a manner*  
8 *that considers the developmental needs of different age*  
9 *ranges of covered minors) to result in reasonably nec-*  
10 *essary and proportionate residual risk to covered mi-*  
11 *nors;*

12           (3) *mitigate privacy risks, including substantial*  
13 *privacy risks, related to the products and services of*  
14 *the covered entity or the service provider, including in*  
15 *the design, development, and implementation of such*  
16 *products and services, taking into account the role of*  
17 *the covered entity or service provider and the infor-*  
18 *mation available to it; and*

19           (4) *implement reasonable training and safe-*  
20 *guards within the covered entity and service provider*  
21 *to promote compliance with all privacy laws applica-*  
22 *ble to covered data the covered entity collects, proc-*  
23 *esses, or transfers or covered data the service provider*  
24 *collects, processes, or transfers on behalf of the covered*  
25 *entity and mitigate privacy risks, including substan-*

1        *tial privacy risks, taking into account the role of the*  
2        *covered entity or service provider and the information*  
3        *available to it.*

4        *(b) FACTORS TO CONSIDER.—The policies, practices,*  
5        *and procedures established by a covered entity and a service*  
6        *provider under subsection (a), shall correspond with, as ap-*  
7        *plicable—*

8                *(1) the size of the covered entity or the service*  
9                *provider and the nature, scope, and complexity of the*  
10               *activities engaged in by the covered entity or service*  
11               *provider, including whether the covered entity or serv-*  
12               *ice provider is a large data holder, nonprofit organi-*  
13               *zation, entity meeting the requirements of section 209,*  
14               *third party, or third-party collecting entity, taking*  
15               *into account the role of the covered entity or service*  
16               *provider and the information available to it;*

17               *(2) the sensitivity of the covered data collected,*  
18               *processed, or transferred by the covered entity or serv-*  
19               *ice provider;*

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

23               *(4) the number of individuals and devices to*  
24               *which the covered data collected, processed, or trans-*

1       ferred by the covered entity or service provider relates;  
2       and

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

6       (c) *COMMISSION GUIDANCE.*—Not later than 1 year  
7 after the date of enactment of this Act, the Commission shall  
8 issue guidance as to what constitutes reasonable policies,  
9 practices, and procedures as required by this section. The  
10 Commission shall consider unique circumstances applicable  
11 to nonprofit organizations, to entities meeting the require-  
12 ments of section 209, and to service providers.

13 **SEC. 104. LOYALTY TO INDIVIDUALS WITH RESPECT TO**  
14                               **PRICING.**

15       (a) *RETALIATION THROUGH SERVICE OR PRICING*  
16 *PROHIBITED.*—A covered entity may not retaliate against  
17 an individual for exercising any of the rights guaranteed  
18 by the Act, or any regulations promulgated under this Act,  
19 including denying goods or services, charging different  
20 prices or rates for goods or services, or providing a different  
21 level of quality of goods or services.

22       (b) *RULES OF CONSTRUCTION.*—Nothing in subsection  
23 (a) may be construed to—

24               (1) prohibit the relation of the price of a service  
25       or the level of service provided to an individual to the

1        *provision, by the individual, of financial information*  
2        *that is necessarily collected and processed only for the*  
3        *purpose of initiating, rendering, billing for, or col-*  
4        *lecting payment for a service or product requested by*  
5        *the individual;*

6            *(2) prohibit a covered entity from offering a dif-*  
7        *ferent price, rate, level, quality or selection of goods*  
8        *or services to an individual, including offering goods*  
9        *or services for no fee, if the offering is in connection*  
10       *with an individual's voluntary participation in a*  
11       *bona fide loyalty program;*

12           *(3) require a covered entity to provide a bona*  
13       *fide loyalty program that would require the covered*  
14       *entity to collect, process, or transfer covered data that*  
15       *the covered entity otherwise would not collect, process,*  
16       *or transfer;*

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

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

24           *(6) prohibit a covered entity from declining to*  
25       *provide a product or service insofar as the collection*



1        *and processing of covered data is strictly necessary*  
2        *for such product or service.*

3        *(c) BONA FIDE LOYALTY PROGRAM DEFINED.—For*  
4        *purposes of this section, the term “bona fide loyalty pro-*  
5        *gram” includes rewards, premium features, discount or club*  
6        *card programs.*

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

9        **SEC. 201. CONSUMER AWARENESS.**

10        *(a) IN GENERAL.—Not later than 90 days after the*  
11        *date of enactment of this Act, the Commission shall publish,*  
12        *on the public website of the Commission, a webpage that*  
13        *describes each provision, right, obligation, and requirement*  
14        *of this Act, listed separately for individuals and for covered*  
15        *entities and service providers, and the remedies, exemp-*  
16        *tions, and protections associated with this Act, in plain and*  
17        *concise language and in an easy-to-understand manner.*

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

22        *(c) ACCESSIBILITY.—The Commission shall publish*  
23        *the information required to be published under subsection*  
24        *(a) in the ten languages with the most users in the United*  
25        *States, according to the most recent United States Census.*

1 **SEC. 202. TRANSPARENCY.**

2 (a) *IN GENERAL.*—Each covered entity shall make  
3 publicly available, in a clear, conspicuous, not misleading,  
4 and easy-to-read and readily accessible manner, a privacy  
5 policy that provides a detailed and accurate representation  
6 of the data collection, processing, and transfer activities of  
7 the covered entity.

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

11 (1) *The identity and the contact information*  
12 *of—*

13 (A) *the covered entity or service provider to*  
14 *which the privacy policy applies (including the*  
15 *covered entity’s or service provider’s points of*  
16 *contact and generic electronic mail addresses, as*  
17 *applicable for privacy and data security inquir-*  
18 *ies); and*

19 (B) *any other entity within the same cor-*  
20 *porate structure as the covered entity or service*  
21 *provider to which covered data is transferred by*  
22 *the covered entity.*

23 (2) *The categories of covered data the covered en-*  
24 *tity or service provider collects or processes.*

1           (3) *The processing purposes for each category of*  
2           *covered data the covered entity or service provider col-*  
3           *lects or processes.*

4           (4) *Whether the covered entity or service provider*  
5           *transfers covered data and, if so, each category of*  
6           *service provider and third party to which the covered*  
7           *entity or service provider transfers covered data, the*  
8           *name of each third-party collecting entity to which*  
9           *the covered entity or service provider transfers covered*  
10          *data, and the purposes for which such data is trans-*  
11          *ferred to such categories of service providers and third*  
12          *parties or third-party collecting entities, except for a*  
13          *transfer to a governmental entity pursuant to a court*  
14          *order or law that prohibits the covered entity or serv-*  
15          *ice provider from disclosing such transfer, except for*  
16          *transfers to governmental entities pursuant to a court*  
17          *order or law that prohibits the covered entity from*  
18          *disclosing the transfer.*

19          (5) *The length of time the covered entity or serv-*  
20          *ice provider intends to retain each category of covered*  
21          *data, including sensitive covered data, or, if it is not*  
22          *possible to identify that timeframe, the criteria used*  
23          *to determine the length of time the covered entity or*  
24          *service provider intends to retain categories of covered*  
25          *data.*

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

3           (7) *A general description of the covered entity's*  
4           *or service provider's data security practices.*

5           (8) *The effective date of the privacy policy.*

6           (9) *Whether or not any covered data collected by*  
7           *the covered entity or service provider is transferred to,*  
8           *processed in, stored in, or otherwise accessible to the*  
9           *People's Republic of China, Russia, Iran, or North*  
10          *Korea.*

11          (c) *LANGUAGES.—The privacy policy required under*  
12          *subsection (a) shall be made available to the public in each*  
13          *covered language in which the covered entity or service pro-*  
14          *vider—*

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

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

19          (d) *ACCESSIBILITY.—The covered entity or service pro-*  
20          *vider shall also provide the disclosures under this section*  
21          *in a manner that is reasonably accessible to and usable by*  
22          *individuals with disabilities.*

23          (e) *MATERIAL CHANGES.—*

24                 (1) *AFFIRMATIVE EXPRESS CONSENT.—If a cov-*  
25                 *ered entity makes a material change to its privacy*

1        *policy or practices, the covered entity shall notify*  
2        *each individual affected by such material change be-*  
3        *fore implementing the material change with respect to*  
4        *any prospectively collected covered data and, except*  
5        *as provided in paragraphs (1) through (15) of section*  
6        *101(b), provide a reasonable opportunity for each in-*  
7        *dividual to withdraw consent to any further materi-*  
8        *ally different collection, processing, or transfer of pre-*  
9        *viously collected covered data under the changed pol-*  
10       *icy.*

11            (2) *NOTIFICATION.*—*The covered entity shall take*  
12        *all reasonable electronic measures to provide direct*  
13        *notification regarding material changes to the pri-*  
14        *vacancy policy to each affected individual, in each cov-*  
15        *ered language in which the privacy policy is made*  
16        *available, and taking into account available tech-*  
17        *nology and the nature of the relationship.*

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

21            (4) *LOG OF MATERIAL CHANGES.*—*Each large*  
22        *data holder shall retain copies of previous versions of*  
23        *its privacy policy for at least 10 years beginning*  
24        *after the date of enactment of this Act and publish*  
25        *them on its website. Such large data holder shall*

1        *make publicly available, in a clear, conspicuous, and*  
2        *readily accessible manner, a log describing the date*  
3        *and nature of each material change to its privacy*  
4        *policy over the past 10 years. The descriptions shall*  
5        *be sufficient for a reasonable individual to under-*  
6        *stand the material effect of each material change. The*  
7        *obligations in this paragraph shall not apply to any*  
8        *previous versions of a large data holder’s privacy pol-*  
9        *icy, or any material changes to such policy, that pre-*  
10       *cede the date of enactment of this Act.*

11       *(f) SHORT-FORM NOTICE TO CONSUMERS BY LARGE*  
12       *DATA HOLDERS.—*

13                *(1) IN GENERAL.—In addition to the privacy*  
14        *policy required under subsection (a), a large data*  
15        *holder that is a covered entity shall provide a short-*  
16        *form notice of its covered data practices in a manner*  
17        *that is—*

18                        *(A) concise, clear, conspicuous, and not*  
19        *misleading;*

20                        *(B) readily accessible to the individual,*  
21        *based on what is reasonably anticipated within*  
22        *the context of the relationship between the indi-*  
23        *vidual and the large data holder;*

24                        *(C) inclusive of an overview of individual*  
25        *rights and disclosures to reasonably draw atten-*

1           tion to data practices that may reasonably be  
2           unexpected to a reasonable person or that involve  
3           sensitive covered data; and

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

5           (2) *RULEMAKING.*—The Commission shall issue  
6           a rule pursuant to section 553 of title 5, United  
7           States Code, establishing the minimum data disclo-  
8           sures necessary for the short-form notice required  
9           under paragraph (1), which shall not exceed the con-  
10          tent requirements in subsection (b) and shall include  
11          templates or models of short-form notices.

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

13          (a) *ACCESS TO, AND CORRECTION, DELETION, AND*  
14 *PORTABILITY OF, COVERED DATA.*—In accordance with  
15 subsections (b) and (c), a covered entity shall provide an  
16 individual, after receiving a verified request from the indi-  
17 vidual, with the right to—

18                   (1) access—

19                           (A) in a human-readable format that a rea-  
20                           sonable individual can understand and  
21                           download from the internet, the covered data (ex-  
22                           cept covered data in a back-up or archival sys-  
23                           tem) of the individual making the request that is  
24                           collected, processed, or transferred by the covered

1            *entity or any service provider of the covered enti-*  
2            *ty within the 24 months preceding the request;*

3            *(B) the categories of any third party, if ap-*  
4            *plicable, and an option for consumers to obtain*  
5            *the names of any such third party as well as and*  
6            *the categories of any service providers to whom*  
7            *the covered entity has transferred for consider-*  
8            *ation the covered data of the individual, as well*  
9            *as the categories of sources from which the cov-*  
10           *ered data was collected; and*

11           *(C) a description of the purpose for which*  
12           *the covered entity transferred the covered data of*  
13           *the individual to a third party or service pro-*  
14           *vider;*

15           *(2) correct any verifiable substantial inaccuracy*  
16           *or substantially incomplete information with respect*  
17           *to the covered data of the individual that is processed*  
18           *by the covered entity and instruct the covered entity*  
19           *to make reasonable efforts to notify all third parties*  
20           *or service providers to which the covered entity trans-*  
21           *ferred such covered data of the corrected information;*

22           *(3) delete covered data of the individual that is*  
23           *processed by the covered entity and instruct the cov-*  
24           *ered entity to make reasonable efforts to notify all*  
25           *third parties or service provider to which the covered*



1        *entity transferred such covered data of the individ-*  
2        *ual's deletion request; and*

3            *(4) to the extent technically feasible, export to the*  
4        *individual or directly to another entity the covered*  
5        *data of the individual that is processed by the covered*  
6        *entity, including inferences linked or reasonably*  
7        *linkable to the individual but not including other de-*  
8        *derived data, without licensing restrictions that limit*  
9        *such transfers in—*

10            *(A) a human-readable format that a reason-*  
11        *able individual can understand and download*  
12        *from the internet; and*

13            *(B) a portable, structured, interoperable,*  
14        *and machine-readable format.*

15        *(b) INDIVIDUAL AUTONOMY.—A covered entity may*  
16        *not condition, effectively condition, attempt to condition,*  
17        *or attempt to effectively condition the exercise of a right*  
18        *described in subsection (a) through—*

19            *(1) the use of any false, fictitious, fraudulent, or*  
20        *materially misleading statement or representation; or*

21            *(2) the design, modification, or manipulation of*  
22        *any user interface with the purpose or substantial ef-*  
23        *fect of obscuring, subverting, or impairing a reason-*  
24        *able individual's autonomy, decision making, or*  
25        *choice to exercise such right.*

1       (c) *TIMING.*—

2           (1) *IN GENERAL.*—*Subject to subsections (d) and*  
3 *(e), each request under subsection (a) shall be com-*  
4 *pleted by any—*

5           (A) *large data holder within 45 days of*  
6 *such request from an individual, unless it is de-*  
7 *monstrably impracticable or impracticably costly*  
8 *to verify such individual;*

9           (B) *covered entity that is not a large data*  
10 *holder or a covered entity meeting the require-*  
11 *ments of section 209 within 60 days of such re-*  
12 *quest from an individual, unless it is demon-*  
13 *strably impracticable or impracticably costly to*  
14 *verify such individual; or*

15           (C) *covered entity meeting the requirements*  
16 *of section 209 within 90 days of such request*  
17 *from an individual, unless it is demonstrably*  
18 *impracticable or impracticably costly to verify*  
19 *such individual.*

20           (2) *EXTENSION.*—*A response period set forth in*  
21 *this subsection may be extended once by 45 additional*  
22 *days when reasonably necessary, considering the com-*  
23 *plexity and number of the individual's requests, so*  
24 *long as the covered entity informs the individual of*

1        *any such extension within the initial 45-day response*  
2        *period, together with the reason for the extension.*

3        *(d) FREQUENCY AND COST OF ACCESS.—A covered en-*  
4        *tity—*

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

8                *(2) with respect to—*

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

13                        *(B) any time beyond the initial 2 times de-*  
14        *scribed in subparagraph (A), may allow the in-*  
15        *dividual to exercise such right for a reasonable*  
16        *fee for each request.*

17        *(e) VERIFICATION AND EXCEPTIONS.—*

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

22                        *(A) cannot reasonably verify that the indi-*  
23        *vidual making the request to exercise the right is*  
24        *the individual whose covered data is the subject*

1           *of the request or an individual authorized to*  
2           *make such a request on the individual's behalf;*

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

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

9           *(D) reasonably believes that the exercise of*  
10          *the right would require the covered entity to en-*  
11          *gage in an unfair or deceptive practice under*  
12          *section 5 of the Federal Trade Commission Act*  
13          *(15 U.S.C. 45); or*

14          *(E) reasonably believes that the request is*  
15          *made to further fraud, support criminal activity,*  
16          *or the exercise of the right presents a data secu-*  
17          *rity threat.*

18          *(2) ADDITIONAL INFORMATION.—If a covered en-*  
19          *tity cannot reasonably verify that a request to exer-*  
20          *cise a right described in subsection (a) is made by the*  
21          *individual whose covered data is the subject of the re-*  
22          *quest (or an individual authorized to make such a re-*  
23          *quest on the individual's behalf), the covered entity—*

24                  *(A) may request that the individual making*  
25                  *the request to exercise the right provide any ad-*

1           *ditional information necessary for the sole pur-*  
2           *pose of verifying the identity of the individual;*  
3           *and*

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

6           (3) *PERMISSIVE EXCEPTIONS.—*

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

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

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

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

1                   (iv) require the covered entity to main-  
2                   tain covered data in an identifiable form or  
3                   collect, retain, or access any data in order  
4                   to be capable of associating a verified indi-  
5                   vidual request with covered data of such in-  
6                   dividual;

7                   (v) result in the release of trade secrets  
8                   or other privileged or confidential business  
9                   information;

10                  (vi) require the covered entity to cor-  
11                  rect any covered data that cannot be reason-  
12                  ably verified as being inaccurate or incom-  
13                  plete;

14                  (vii) interfere with law enforcement,  
15                  judicial proceedings, investigations, or rea-  
16                  sonable efforts to guard against, detect, pre-  
17                  vent, or investigate fraudulent, malicious,  
18                  or unlawful activity, or enforce valid con-  
19                  tracts;

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

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

1           *of deletion requests, maintained solely for*  
2           *the purpose of preventing covered data of an*  
3           *individual from being recollected after the*  
4           *individual submitted a deletion request and*  
5           *requested that the covered entity no longer*  
6           *collect, process, or transfer such data;*

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

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

13                           *(I) unreasonably interfere with*  
14                           *the provision of products or services by*  
15                           *the covered entity to another person it*  
16                           *currently serves;*

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

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

1                   (IV) delete covered data that the  
2 covered entity needs to retain in order  
3 to comply with professional ethical ob-  
4 ligations;

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

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

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



1           (C) *NUMBER OF REQUESTS.*—For purposes  
2           of subparagraph (A)(ii), the receipt of a large  
3           number of verified requests, on its own, may not  
4           be considered to render compliance with a re-  
5           quest demonstrably impracticable.

6           (D) *FURTHER EXCEPTIONS.*—The Commis-  
7           sion may, by regulation as described in sub-  
8           section (g), establish additional permissive excep-  
9           tions necessary to protect the rights of individ-  
10          uals, alleviate undue burdens on covered entities,  
11          prevent unjust or unreasonable outcomes from  
12          the exercise of access, correction, deletion, or  
13          portability rights, or as otherwise necessary to  
14          fulfill the purposes of this section. In establishing  
15          such exceptions, the Commission should consider  
16          any relevant changes in technology, means for  
17          protecting privacy and other rights, and bene-  
18          ficial uses of covered data by covered entities.

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

23               (1) *Compile the following metrics for the prior*  
24               *calendar year:*

1           (A) *The number of verified access requests*  
2           *under subsection (a)(1).*

3           (B) *The number of verified deletion requests*  
4           *under subsection (a)(3).*

5           (C) *The number of requests to opt-out of*  
6           *covered data transfers under section 204(b).*

7           (D) *The number of requests to opt-out of*  
8           *targeted advertising under section 204(c).*

9           (E) *The number of requests in each of sub-*  
10          *paragraphs (A) through (D) that such large data*  
11          *holder (i) complied with in whole or in part and*  
12          *(ii) denied.*

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

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

23          (g) *REGULATIONS.—Not later than 2 years after the*  
24          *date of enactment of this Act, the Commission shall promul-*  
25          *gate regulations, pursuant to section 553 of title 5, United*

1 *States Code, as necessary to establish processes by which*  
2 *covered entities are to comply with the provisions of this*  
3 *section. Such regulations shall take into consideration—*

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

10           (2) *the sensitivity of covered data collected, proc-*  
11 *essed, or transferred by the covered entity;*

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

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

17           (5) *after consulting the National Institute of*  
18 *Standards and Technology, standards for ensuring*  
19 *the deletion of covered data under this Act where ap-*  
20 *propriate.*

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

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

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

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

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

13 *(1) IN GENERAL.—A covered entity—*

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

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

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

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

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

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

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

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

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

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

1        *vider to serve, deliver, or otherwise handle the adver-*  
2        *tisement of the opt-out decision.*

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

7            *(1) the use of any false, fictitious, fraudulent, or*  
8            *materially misleading statement or representation; or*

9            *(2) the design, modification, or manipulation of*  
10          *any user interface with the purpose or substantial ef-*  
11          *fect of obscuring, subverting, or impairing a reason-*  
12          *able individual’s autonomy, decision making, or*  
13          *choice to exercise any such right.*

14        **SEC. 205. DATA PROTECTIONS FOR CHILDREN AND MINORS.**

15          *(a) PROHIBITION ON TARGETED ADVERTISING TO*  
16          *CHILDREN AND MINORS.—A covered entity may not engage*  
17          *in targeted advertising to any individual if the covered en-*  
18          *tity has knowledge that the individual is a covered minor.*

19          *(b) DATA TRANSFER REQUIREMENTS RELATED TO*  
20          *COVERED MINORS.—*

21            *(1) IN GENERAL.—A covered entity may not*  
22            *transfer or direct the transfer of the covered data of*  
23            *a covered minor to a third party if the covered enti-*  
24            *ty—*

1           (A) has knowledge that the individual is a  
2 covered minor; and

3           (B) has not obtained affirmative express  
4 consent from the covered minor or the covered  
5 minor's parent or guardian.

6           (2) *EXCEPTION.*—A covered entity or service pro-  
7 vider may collect, process, or transfer covered data of  
8 an individual the covered entity or service provider  
9 knows is under the age of 18 solely in order to submit  
10 information relating to child victimization to law en-  
11 forcement or to the nonprofit, national resource center  
12 and clearinghouse congressionally designated to pro-  
13 vide assistance to victims, families, child-serving pro-  
14 fessionals, and the general public on missing and ex-  
15 ploited children issues.

16           (c) *YOUTH PRIVACY AND MARKETING DIVISION.*—

17           (1) *ESTABLISHMENT.*—There is established with-  
18 in the Commission in the privacy bureau established  
19 in this Act, a division to be known as the “Youth Pri-  
20 vacy and Marketing Division” (in this section re-  
21 ferred to as the “Division”).

22           (2) *DIRECTOR.*—The Division shall be headed by  
23 a Director, who shall be appointed by the Chair of the  
24 Commission.

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

4                     (A) *the privacy of children and minors; and*  
5                     (B) *marketing directed at children and mi-*  
6           *nors.*

7           (4) *STAFF.*—*The Director of the Division shall*  
8           *hire adequate staff to carry out the duties described*  
9           *in paragraph (3), including by hiring individuals*  
10           *who are experts in data protection, digital adver-*  
11           *tising, data analytics, and youth development.*

12           (5) *REPORTS.*—*Not later than 2 years after the*  
13           *date of enactment of this Act, and annually there-*  
14           *after, the Commission shall submit to the Committee*  
15           *on Commerce, Science, and Transportation of the*  
16           *Senate and the Committee on Energy and Commerce*  
17           *of the House of Representatives a report that in-*  
18           *cludes—*

19                     (A) *a description of the work of the Divi-*  
20                     *sion regarding emerging concerns relating to*  
21                     *youth privacy and marketing practices; and*

22                     (B) *an assessment of how effectively the Di-*  
23                     *vision has, during the period for which the re-*  
24                     *port is submitted, assisted the Commission to ad-*  
25                     *dress youth privacy and marketing practices.*



1           (6) *PUBLICATION.*—Not later than 10 days after  
2           the date on which a report is submitted under para-  
3           graph (5), the Commission shall publish the report on  
4           its website.

5           (d) *REPORT BY THE INSPECTOR GENERAL.*—

6           (1) *IN GENERAL.*—Not later than 2 years after  
7           the date of enactment of this Act, and biennially  
8           thereafter, the Inspector General of the Commission  
9           shall submit to the Commission and to the Committee  
10          on Commerce, Science, and Transportation of the  
11          Senate and the Committee on Energy and Commerce  
12          of the House of Representatives a report regarding the  
13          safe harbor provisions in section 1304 of the Chil-  
14          dren’s Online Privacy Protection Act of 1998 (15  
15          U.S.C. 6503), which shall include—

16                (A) an analysis of whether the safe harbor  
17                provisions are—

18                       (i) operating fairly and effectively; and

19                       (ii) effectively protecting the interests  
20                       of children and minors; and

21                (B) any proposal or recommendation for  
22                policy changes that would improve the effective-  
23                ness of the safe harbor provisions.

24           (2) *PUBLICATION.*—Not later than 10 days after  
25           the date on which a report is submitted under para-

1        *graph (1), the Commission shall publish the report on*  
2        *the website of the Commission.*

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

4        *(a) NOTICE.—Each third-party collecting entity shall*  
5        *place a clear, conspicuous, not misleading, and readily ac-*  
6        *cessible notice on the website or mobile application of the*  
7        *third-party collecting entity (if the third-party collecting*  
8        *entity maintains such a website or mobile application)*  
9        *that—*

10                *(1) notifies individuals that the entity is a third-*  
11                *party collecting entity using specific language that*  
12                *the Commission shall develop through rulemaking*  
13                *under section 553 of title 5, United States Code;*

14                *(2) includes a link to the website established*  
15                *under subsection (b)(3); and*

16                *(3) is reasonably accessible to and usable by in-*  
17                *dividuals with disabilities.*

18        *(b) THIRD-PARTY COLLECTING ENTITY REGISTRA-*  
19        *TION.—*

20                *(1) IN GENERAL.—Not later than January 31 of*  
21                *each calendar year that follows a calendar year dur-*  
22                *ing which a covered entity acted as a third-party col-*  
23                *lecting entity and processed covered data pertaining*  
24                *to more than 5,000 individuals or devices that iden-*  
25                *tify or are linked or reasonably linkable to an indi-*

1        *vidual, such covered entity shall register with the*  
2        *Commission in accordance with this subsection.*

3            (2) *REGISTRATION REQUIREMENTS.—In reg-*  
4        *istering with the Commission as required under para-*  
5        *graph (1), a third-party collecting entity shall do the*  
6        *following:*

7            (A) *Pay to the Commission a registration*  
8        *fee of \$100.*

9            (B) *Provide the Commission with the fol-*  
10       *lowing information:*

11            (i) *The legal name and primary phys-*  
12        *ical, email, and internet addresses of the*  
13        *third-party collecting entity.*

14            (ii) *A description of the categories of*  
15        *covered data the third-party collecting enti-*  
16        *ty processes and transfers.*

17            (iii) *The contact information of the*  
18        *third-party collecting entity, including a*  
19        *contact person, a telephone number, an e-*  
20        *mail address, a website, and a physical*  
21        *mailing address.*

22            (iv) *A link to a website through which*  
23        *an individual may easily exercise the rights*  
24        *provided under this subsection.*

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

7           (A) *A listing of all registered third-party*  
8 *collecting entities and a search feature that al-*  
9 *lows members of the public to identify individual*  
10 *third-party collecting entities.*

11           (B) *For each registered third-party col-*  
12 *lecting entity, the information provided under*  
13 *paragraph (2)(B).*

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

23           (I) *delete all covered data related to*  
24 *such individual that the third-party col-*  
25 *lecting entity did not collect from such indi-*

1                    *vidual directly or when acting as a service*  
2                    *provider; and*

3                    *(II) ensure that the third-party col-*  
4                    *lecting entity no longer collects covered data*  
5                    *related to such individual without the af-*  
6                    *firmative express consent of such indi-*  
7                    *vidual, except insofar as the third-party col-*  
8                    *lecting entity is acting as a service pro-*  
9                    *vider.*

10                  *(ii) Each third-party collecting entity that*  
11                  *receives such a request from an individual shall*  
12                  *delete all the covered data of the individual not*  
13                  *later than 30 days after the request is received*  
14                  *by the third-party collecting entity.*

15                  *(iii) Notwithstanding the provisions of*  
16                  *clauses (i) and (ii), a third-party collecting enti-*  
17                  *ty may decline to fulfill a “Do Not Collect” re-*  
18                  *quest from an individual who it has actual*  
19                  *knowledge has been convicted of a crime related*  
20                  *to the abduction or sexual exploitation of a child,*  
21                  *and the data the entity is collecting is necessary*  
22                  *to effectuate the purposes of a national or State-*  
23                  *run sex offender registry or the congressionally*  
24                  *designated entity that serves as the nonprofit na-*  
25                  *tional resource center and clearinghouse to pro-*

1           *vide assistance to victims, families, child-serving*  
2           *professionals, and the general public on missing*  
3           *and exploited children issues.*

4           *(c) PENALTIES.—*

5           *(1) IN GENERAL.—A third-party collecting entity*  
6           *that fails to register or provide the notice as required*  
7           *under this section shall be liable for—*

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

12                   *(B) an amount equal to the registration fees*  
13                   *due under paragraph (2)(A) of subsection (b) for*  
14                   *each year that the third-party collecting entity*  
15                   *failed to register as required under paragraph*  
16                   *(1) of such subsection.*

17           *(2) RULE OF CONSTRUCTION.—Nothing in this*  
18           *subsection shall be construed as altering, limiting, or*  
19           *affecting any enforcement authorities or remedies*  
20           *under this Act.*

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

22           *(a) CIVIL RIGHTS PROTECTIONS.—*

23           *(1) IN GENERAL.—A covered entity or a service*  
24           *provider may not collect, process, or transfer covered*  
25           *data in a manner that discriminates in or otherwise*

1       *makes unavailable the equal enjoyment of goods or*  
2       *services on the basis of race, color, religion, national*  
3       *origin, sex, or disability.*

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

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

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

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

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

16       (b) *FTC ENFORCEMENT ASSISTANCE.—*

17           (1) *IN GENERAL.—Whenever the Commission ob-*  
18       *tains information that a covered entity or service pro-*  
19       *vider may have collected, processed, or transferred*  
20       *covered data in violation of subsection (a), the Com-*  
21       *mission shall transmit such information as allowable*  
22       *under Federal law to any Executive agency with au-*  
23       *thority to initiate enforcement actions or proceedings*  
24       *relating to such violation.*

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

5                   (A) *the types of information the Commis-*  
6 *sion transmitted to Executive agencies under*  
7 *paragraph (1) during the previous 1-year period;*  
8 *and*

9                   (B) *how such information relates to Federal*  
10 *civil rights laws.*

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

16           (4) *COOPERATION WITH OTHER AGENCIES.*—*The*  
17 *Commission may implement this subsection by exe-*  
18 *cuting agreements or memoranda of understanding*  
19 *with the appropriate Executive agencies.*

20           (c) *COVERED ALGORITHM IMPACT AND EVALUA-*  
21 *TION.*—

22                   (1) *COVERED ALGORITHM IMPACT ASSESS-*  
23 *MENT.*—

24                           (A) *IMPACT ASSESSMENT.*—*Notwith-*  
25 *standing any other provision of law, not later*



1           *than 2 years after the date of enactment of this*  
2           *Act, and annually thereafter, a large data holder*  
3           *that uses a covered algorithm in a manner that*  
4           *poses a consequential risk of harm to an indi-*  
5           *vidual or group of individuals, and uses such*  
6           *covered algorithm solely or in part, to collect,*  
7           *process, or transfer covered data shall conduct an*  
8           *impact assessment of such algorithm in accord-*  
9           *ance with subparagraph (B).*

10           *(B) IMPACT ASSESSMENT SCOPE.—The im-*  
11            *pact assessment required under subparagraph*  
12           *(A) shall provide the following:*

13                   *(i) A detailed description of the design*  
14                   *process and methodologies of the covered al-*  
15                   *gorithm.*

16                   *(ii) A statement of the purpose and*  
17                   *proposed uses of the covered algorithm.*

18                   *(iii) A detailed description of the data*  
19                   *used by the covered algorithm, including the*  
20                   *specific categories of data that will be proc-*  
21                   *essed as input and any data used to train*  
22                   *the model that the covered algorithm relies*  
23                   *on, if applicable.*

24                   *(iv) A description of the outputs pro-*  
25                   *duced by the covered algorithm.*

1                   (v) *An assessment of the necessity and*  
2                   *proportionality of the covered algorithm in*  
3                   *relation to its stated purpose.*

4                   (vi) *A detailed description of steps the*  
5                   *large data holder has taken or will take to*  
6                   *mitigate potential harms from the covered*  
7                   *algorithm to an individual or group of in-*  
8                   *dividuals, including related to—*

9                               (I) *covered minors;*

10                               (II) *making or facilitating adver-*  
11                               *tising for, or determining access to, or*  
12                               *restrictions on the use of housing, edu-*  
13                               *cation, employment, healthcare, insur-*  
14                               *ance, or credit opportunities;*

15                               (III) *determining access to, or re-*  
16                               *strictions on the use of, any place of*  
17                               *public accommodation, particularly as*  
18                               *such harms relate to the protected char-*  
19                               *acteristics of individuals, including*  
20                               *race, color, religion, national origin,*  
21                               *sex, or disability;*

22                               (IV) *disparate impact on the basis*  
23                               *of individuals' race, color, religion, na-*  
24                               *tional origin, sex, or disability status;*  
25                               *or*

1                                   (V) *disparate impact on the basis*  
2                                   *of individuals' political party registra-*  
3                                   *tion status.*

4                   (2) *ALGORITHM DESIGN EVALUATION.—Notwith-*  
5                   *standing any other provision of law, not later than*  
6                   *2 years after the date of enactment of this Act, a cov-*  
7                   *ered entity or service provider that knowingly devel-*  
8                   *ops a covered algorithm that is designed to, solely or*  
9                   *in part, to collect, process, or transfer covered data in*  
10                  *furtherance of a consequential decision shall prior to*  
11                  *deploying the covered algorithm in interstate com-*  
12                  *merce evaluate the design, structure, and inputs of the*  
13                  *covered algorithm, including any training data used*  
14                  *to develop the covered algorithm, to reduce the risk of*  
15                  *the potential harms identified under paragraph*  
16                  *(1)(B).*

17                  (3) *OTHER CONSIDERATIONS.—*

18                       (A) *FOCUS.—In complying with para-*  
19                       *graphs (1) and (2), a covered entity and a serv-*  
20                       *ice provider may focus the impact assessment or*  
21                       *evaluation on any covered algorithm, or portions*  
22                       *of a covered algorithm, that will be put to use*  
23                       *and may reasonably contribute to the risk of the*  
24                       *potential harms identified under paragraph*  
25                       *(1)(B).*

1 (B) AVAILABILITY.—

2 (i) IN GENERAL.—A covered entity and  
3 a service provider—

4 (I) shall, not later than 30 days  
5 after completing an impact assessment  
6 or evaluation, submit the impact as-  
7 sessment or evaluation conducted under  
8 paragraph (1) or (2) to the Commis-  
9 sion;

10 (II) shall, upon request, make  
11 such impact assessment and evaluation  
12 available to Congress; and

13 (III) may make a summary of  
14 such impact assessment and evaluation  
15 publicly available in a place that is  
16 easily accessible to individuals.

17 (ii) TRADE SECRETS.—Covered entities  
18 and service providers may redact and seg-  
19 regate any trade secret (as defined in sec-  
20 tion 1839 of title 18, United States Code) or  
21 other confidential or proprietary informa-  
22 tion from public disclosure under this sub-  
23 paragraph and the Commission shall abide  
24 by its obligations under section 6(f) of the

1                   *Federal Trade Commission Act (15 U.S.C.*  
2                   *46(f)) in regard to such information.*

3                   (C) *ENFORCEMENT.*—*The Commission may*  
4                   *not use any information obtained solely and ex-*  
5                   *clusively through a covered entity or a service*  
6                   *provider’s disclosure of information to the Com-*  
7                   *mission in compliance with this section for any*  
8                   *purpose other than enforcing this Act with the*  
9                   *exception of enforcing consent orders, including*  
10                  *the study and report provisions in paragraph*  
11                  *(6). This subparagraph does not preclude the*  
12                  *Commission from providing this information to*  
13                  *Congress in response to a subpoena.*

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

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

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

4           (B) may exclude from this subsection any  
5           covered algorithm that presents low or minimal  
6           consequential risk of harm to an individual or  
7           group of individuals.

8           (6) *STUDY AND REPORT.*—

9           (A) *STUDY.*—The Commission, in consulta-  
10          tion with the Secretary of Commerce or the Sec-  
11          retary’s designee, shall conduct a study, to re-  
12          view any impact assessment or evaluation sub-  
13          mitted under this subsection. Such study shall  
14          include an examination of—

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

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

20          (B) *REPORT.*—

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

1           *containing the results of the study con-*  
2           *ducted under subparagraph (A), together*  
3           *with recommendations for such legislation*  
4           *and administrative action as the Commis-*  
5           *sion determines appropriate.*

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

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

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

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

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

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

3           (B) *the nature and scope of the covered enti-*  
4           *ty or the service provider's collecting, processing,*  
5           *or transferring of covered data;*

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

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

11          (E) *the current state of the art (and limita-*  
12          *tions thereof) in administrative, technical, and*  
13          *physical safeguards for protecting such covered*  
14          *data; and*

15          (F) *the cost of available tools to improve se-*  
16          *curity and reduce vulnerabilities to unauthorized*  
17          *access and acquisition of such covered data in re-*  
18          *lation to the risks and nature of the covered*  
19          *data.*

20          (b) *SPECIFIC REQUIREMENTS.—The data security*  
21          *practices of the covered entity and of the service provider*  
22          *required under subsection (a) shall include, for each respec-*  
23          *tive entity's own system or systems, at a minimum, the fol-*  
24          *lowing practices:*



1           (1) *ASSESS VULNERABILITIES.*—*Identifying and*  
2           *assessing any material internal and external risk to,*  
3           *and vulnerability in, the security of each system*  
4           *maintained by the covered entity that collects, proc-*  
5           *esses, or transfers covered data, or service provider*  
6           *that collects, processes, or transfers covered data on*  
7           *behalf of the covered entity, including unauthorized*  
8           *access to or risks to such covered data, human*  
9           *vulnerabilities, access rights, and the use of service*  
10           *providers. With respect to large data holders, such ac-*  
11           *tivities shall include a plan to receive and reasonably*  
12           *respond to unsolicited reports of vulnerabilities by*  
13           *any entity or individual and by performing a reason-*  
14           *able investigation of such reports.*

15           (2) *PREVENTIVE AND CORRECTIVE ACTION.*—  
16           *Taking preventive and corrective action designed to*  
17           *mitigate reasonably foreseeable risks or vulnerabilities*  
18           *to covered data identified by the covered entity or*  
19           *service provider, consistent with the nature of such*  
20           *risk or vulnerability and the entity's role in col-*  
21           *lecting, processing, or transferring the data. Such ac-*  
22           *tion may include implementing administrative, tech-*  
23           *anical, or physical safeguards or changes to data secu-*  
24           *rity practices or the architecture, installation, or im-*

1        *plementation of network or operating software, among*  
2        *other actions.*

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

10               (4) *INFORMATION RETENTION AND DISPOSAL.—*  
11        *Disposing of covered data in accordance with a reten-*  
12        *tion schedule that shall require the deletion of covered*  
13        *data when such data is required to be deleted by law*  
14        *or is no longer necessary for the purpose for which the*  
15        *data was collected, processed, or transferred, unless an*  
16        *individual has provided affirmative express consent to*  
17        *such retention. Such disposal shall include destroying,*  
18        *permanently erasing, or otherwise modifying the cov-*  
19        *ered data to make such data permanently unreadable*  
20        *or indecipherable and unrecoverable to ensure ongoing*  
21        *compliance with this section. Service providers shall*  
22        *establish practices to delete or return covered data to*  
23        *a covered entity as requested at the end of the provi-*  
24        *sion of services unless retention of the covered data is*  
25        *required by law, consistent with section 302(a)(6).*

1           (5) *TRAINING.*—*Training each employee with ac-*  
2           *cess to covered data on how to safeguard covered data*  
3           *and updating such training as necessary.*

4           (6) *DESIGNATION.*—*Designating an officer, em-*  
5           *ployee, or employees to maintain and implement such*  
6           *practices.*

7           (7) *INCIDENT RESPONSE.*—*Implementing proce-*  
8           *dures to detect, respond to, or recover from security*  
9           *incidents, including breaches.*

10          (c) *REGULATIONS.*—*The Commission may promulgate,*  
11          *in accordance with section 553 of title 5, United States*  
12          *Code, technology-neutral regulations to establish processes*  
13          *for complying with this section. The Commission shall con-*  
14          *sult with the National Institute of Standards and Tech-*  
15          *nology in establishing such processes.*

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

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

23                  (1) *be exempt from compliance with section*  
24                  *203(a)(4), paragraphs (1) through (3) and (5)*  
25                  *through (7) of section 208(b), and section 301(c); and*

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

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

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

13           (2) *The covered entity or service provider, on av-*  
14 *erage, did not annually collect or process the covered*  
15 *data of more than 200,000 individuals during the pe-*  
16 *riod beyond the purpose of initiating, rendering, bill-*  
17 *ing for, finalizing, completing, or otherwise collecting*  
18 *payment for a requested service or product, so long as*  
19 *all covered data for such purpose was deleted or de-*  
20 *identified within 90 days, except when necessary to*  
21 *investigate fraud or as consistent with a covered enti-*  
22 *ty's return policy.*

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

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

3        *(c) REVENUE DEFINED.—For purposes of this section,*  
4        *the term “revenue” as it relates to any covered entity or*  
5        *service provider that is not organized to carry on business*  
6        *for its own profit or that of its members, means the gross*  
7        *receipts the covered entity or service provider received in*  
8        *whatever form from all sources without subtracting any*  
9        *costs or expenses, and includes contributions, gifts, grants,*  
10       *dues or other assessments, income from investments, or pro-*  
11       *ceeds from the sale of real or personal property.*

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

13       *(a) IN GENERAL.—For the rights established under*  
14       *subsection (b) of section 204, subsection (c) of section 204*  
15       *(except as provided for under section 101(b)(16)), and sec-*  
16       *tion 206(b)(3)(C), following public notice and opportunity*  
17       *to comment and not later than 18 months after the date*  
18       *of enactment of this Act, the Commission shall establish or*  
19       *recognize one or more acceptable privacy protective, central-*  
20       *ized mechanisms, including global privacy signals such as*  
21       *browser or device privacy settings, other tools offered by cov-*  
22       *ered entities or service providers, and registries of identi-*  
23       *fiers, for individuals to exercise all such rights through a*  
24       *single interface for a covered entity or service provider to*  
25       *utilize to allow an individual to make such opt out designa-*

1 *tions with respect to covered data related to such indi-*  
2 *vidual.*

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

5 *(1) require covered entities or service providers*  
6 *acting on behalf of covered entities to inform individ-*  
7 *uals about the centralized opt-out choice;*

8 *(2) not be required to be the default setting, but*  
9 *may be the default setting provided that in all cases*  
10 *the mechanism clearly represents the individual’s af-*  
11 *firmative, freely given, and unambiguous choice to*  
12 *opt out;*

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

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

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

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

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

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

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

13                  (1) *internal controls reasonably designed to com-*  
14                  *ply with this Act; and*

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

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

1 *reasonable investigation, reasonable ground to believe and*  
2 *did believe, at the time that certification was submitted,*  
3 *that the statements therein were true and that there was*  
4 *no omission to state a material fact required to be stated*  
5 *therein or necessary to make the statements therein not mis-*  
6 *leading.*

7 *(c) DESIGNATION OF PRIVACY AND DATA SECURITY*  
8 *OFFICER.—*

9 *(1) IN GENERAL.—A covered entity or service*  
10 *provider that have more than 15 employees, shall des-*  
11 *ignate—*

12 *(A) 1 or more qualified employees as pri-*  
13 *vacancy officers; and*

14 *(B) 1 or more qualified employees (in addi-*  
15 *tion to any employee designated under subpara-*  
16 *graph (A)) as data security officers.*

17 *(2) REQUIREMENTS FOR OFFICERS.—An em-*  
18 *ployee who is designated by a covered entity or a*  
19 *service provider as a privacy officer or a data secu-*  
20 *rity officer pursuant to paragraph (1) shall, at a*  
21 *minimum—*

22 *(A) implement a data privacy program and*  
23 *data security program to safeguard the privacy*  
24 *and security of covered data in compliance with*  
25 *the requirements of this Act; and*



1                   (B) facilitate the covered entity or service  
2                   provider's ongoing compliance with this Act.

3                   (3) *ADDITIONAL REQUIREMENTS FOR LARGE*  
4                   *DATA HOLDERS.*—A large data holder shall designate  
5                   at least 1 of the officers described in paragraph (1)  
6                   to report directly to the highest official at the large  
7                   data holder as a privacy protection officer who shall,  
8                   in addition to the requirements in paragraph (2), ei-  
9                   ther directly or through a supervised designee or des-  
10                  ignees—

11                  (A) establish processes to periodically review  
12                  and update the privacy and security policies,  
13                  practices, and procedures of the large data hold-  
14                  er, as necessary;

15                  (B) conduct biennial and comprehensive au-  
16                  dits to ensure the policies, practices, and proce-  
17                  dures of the large data holder ensure the large  
18                  data holder is in compliance with this Act and  
19                  ensure such audits are accessible to the Commis-  
20                  sion upon request;

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

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

1           *and data security practices undertaken by the*  
2           *large data holder; and*

3                   *(E) serve as the point of contact between the*  
4           *large data holder and enforcement authorities.*

5           *(d) LARGE DATA HOLDER PRIVACY IMPACT ASSESS-*  
6           *MENTS.—*

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

18                   *(2) ASSESSMENT REQUIREMENTS.—A privacy*  
19          *impact assessment required under paragraph (1) shall*  
20          *be—*

21                           *(A) reasonable and appropriate in scope*  
22          *given—*

23                                   *(i) the nature of the covered data col-*  
24                                   *lected, processed, and transferred by the*  
25                                   *large data holder;*

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

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

8                   (B) documented in written form and main-  
9                   tained by the large data holder unless rendered  
10                  out of date by a subsequent assessment conducted  
11                  under paragraph (1); and

12                  (C) approved by the privacy protection offi-  
13                  cer designated in subsection (c)(3) of the large  
14                  data holder, as applicable.

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

22                  (e) *OTHER PRIVACY IMPACT ASSESSMENTS.*—

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

1        *and does not meet the requirements for covered enti-*  
2        *ties under section 209 shall conduct a privacy impact*  
3        *assessment. Such assessment shall weigh the benefits*  
4        *of the covered entity's covered data collecting, proc-*  
5        *essing, and transfer practices that may cause a sub-*  
6        *stantial privacy risk against the potential material*  
7        *adverse consequences of such practices to individual*  
8        *privacy.*

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

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

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

17                                (ii) *the volume of the covered data col-*  
18        *lected, processed, and transferred by the cov-*  
19        *ered entity; and*

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

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

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

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

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

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

12                   (1) *shall adhere to the instructions of a covered*  
13           *entity and only collect, process, and transfer service*  
14           *provider data to the extent necessary and propor-*  
15           *tionate to provide a service requested by the covered*  
16           *entity, as set out in the contract required by sub-*  
17           *section (b), and this paragraph does not require a*  
18           *service provider to collect, process, or transfer covered*  
19           *data if the service provider would not otherwise do so;*

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

1           (3) shall assist a covered entity in responding to  
2 a request made by an individual under section 203  
3 or 204, by either—

4           (A) providing appropriate technical and or-  
5 ganizational measures, taking into account the  
6 nature of the processing and the information rea-  
7 sonably available to the service provider, for the  
8 covered entity to comply with such request for  
9 service provider data; or

10           (B) fulfilling a request by a covered entity  
11 to execute an individual rights request that the  
12 covered entity has determined should be complied  
13 with, by either—

14           (i) complying with the request pursu-  
15 ant to the covered entity's instructions; or

16           (ii) providing written verification to  
17 the covered entity that it does not hold cov-  
18 ered data related to the request, that com-  
19 plying with the request would be incon-  
20 sistent with its legal obligations, or that the  
21 request falls within an exception to section  
22 203 or 204;

23           (4) may engage another service provider for pur-  
24 poses of processing service provider data on behalf of  
25 a covered entity only after providing that covered en-

1        *tity with notice and pursuant to a written contract*  
2        *that requires such other service provider to satisfy the*  
3        *obligations of the service provider with respect to such*  
4        *service provider data, including that the other service*  
5        *provider be treated as a service provider under this*  
6        *Act;*

7                *(5) shall, upon the reasonable request of the cov-*  
8        *ered entity, make available to the covered entity infor-*  
9        *mation necessary to demonstrate the compliance of*  
10        *the service provider with the requirements of this Act,*  
11        *which may include making available a report of an*  
12        *independent assessment arranged by the service pro-*  
13        *vider on terms agreed to by the service provider and*  
14        *the covered entity, providing information necessary to*  
15        *enable the covered entity to conduct and document a*  
16        *privacy impact assessment required by subsection (d)*  
17        *or (e) of section 301, and making available the report*  
18        *required under section 207(c)(2);*

19                *(6) shall, at the covered entity's direction, delete*  
20        *or return all covered data to the covered entity as re-*  
21        *quested at the end of the provision of services, unless*  
22        *retention of the covered data is required by law;*

23                *(7) shall develop, implement, and maintain rea-*  
24        *sonable administrative, technical, and physical safe-*  
25        *guards that are designed to protect the security and*

1       *confidentiality of covered data the service provider*  
2       *processes consistent with section 208; and*

3           (8) *shall allow and cooperate with, reasonable*  
4       *assessments by the covered entity or the covered enti-*  
5       *ty's designated assessor; alternatively, the service pro-*  
6       *vider may arrange for a qualified and independent*  
7       *assessor to conduct an assessment of the service pro-*  
8       *vider's policies and technical and organizational*  
9       *measures in support of the obligations under this Act*  
10       *using an appropriate and accepted control standard*  
11       *or framework and assessment procedure for such as-*  
12       *sessments. The service provider shall provide a report*  
13       *of such assessment to the covered entity upon request.*

14       **(b) CONTRACTS BETWEEN COVERED ENTITIES AND**  
15       **SERVICE PROVIDERS.—**

16           (1) **REQUIREMENTS.—***A person or entity may*  
17       *only act as a service provider pursuant to a written*  
18       *contract between the covered entity and the service*  
19       *provider, or a written contract between one service*  
20       *provider and a second service provider as described*  
21       *under subsection (a)(4), if the contract—*

22           (A) *sets forth the data processing procedures*  
23       *of the service provider with respect to collection,*  
24       *processing, or transfer performed on behalf of the*  
25       *covered entity or service provider;*



1                   (B) clearly sets forth—

2                   (i) instructions for collecting, proc-  
3                   essing, or transferring data;

4                   (ii) the nature and purpose of col-  
5                   lecting, processing, or transferring;

6                   (iii) the type of data subject to col-  
7                   lecting, processing, or transferring;

8                   (iv) the duration of processing; and

9                   (v) the rights and obligations of both  
10                  parties, including a method by which the  
11                  service provider shall notify the covered en-  
12                  tity of material changes to its privacy prac-  
13                  tices;

14                 (C) does not relieve a covered entity or a  
15                 service provider of any requirement or liability  
16                 imposed on such covered entity or service pro-  
17                 vider under this Act; and

18                 (D) prohibits—

19                 (i) collecting, processing, or transfer-  
20                 ring covered data in contravention to sub-  
21                 section (a); and

22                 (ii) combining service provider data  
23                 with covered data which the service provider  
24                 receives from or on behalf of another person  
25                 or persons or collects from the interaction of

1           *the service provider with an individual,*  
2           *provided that such combining is not nec-*  
3           *essary to effectuate a purpose described in*  
4           *paragraphs (1) through (15) of section*  
5           *101(b) and is otherwise permitted under the*  
6           *contract required by this subsection.*

7           (2) *CONTRACT TERMS.—Each service provider*  
8           *shall retain copies of previous contracts entered into*  
9           *in compliance with this subsection with each covered*  
10          *entity to which it provides requested products or serv-*  
11          *ices.*

12          (c) *RELATIONSHIP BETWEEN COVERED ENTITIES AND*  
13          *SERVICE PROVIDERS.—*

14                 (1) *Determining whether a person is acting as a*  
15                 *covered entity or service provider with respect to a*  
16                 *specific processing of covered data is a fact-based de-*  
17                 *termination that depends upon the context in which*  
18                 *such data is processed.*

19                 (2) *A person that is not limited in its processing*  
20                 *of covered data pursuant to the instructions of a cov-*  
21                 *ered entity, or that fails to adhere to such instruc-*  
22                 *tions, is a covered entity and not a service provider*  
23                 *with respect to a specific processing of covered data.*  
24                 *A service provider that continues to adhere to the in-*  
25                 *structions of a covered entity with respect to a specific*

1        *processing of covered data remains a service provider.*  
2        *If a service provider begins, alone or jointly with oth-*  
3        *ers, determining the purposes and means of the proc-*  
4        *essing of covered data, it is a covered entity and not*  
5        *a service provider with respect to the processing of*  
6        *such data.*

7            *(3) A covered entity that transfers covered data*  
8        *to a service provider or a service provider that trans-*  
9        *fers covered data to a covered entity or another service*  
10       *provider, in compliance with the requirements of this*  
11       *Act, is not liable for a violation of this Act by the*  
12       *service provider or covered entity to whom such cov-*  
13       *ered data was transferred, if at the time of transfer-*  
14       *ring such covered data, the covered entity or service*  
15       *provider did not have actual knowledge that the serv-*  
16       *ice provider or covered entity would violate this Act.*

17           *(4) A covered entity or service provider that re-*  
18       *ceives covered data in compliance with the require-*  
19       *ments of this Act is not in violation of this Act as*  
20       *a result of a violation by a covered entity or service*  
21       *provider from which such data was received.*

22       *(d) THIRD PARTIES.—A third party—*

23           *(1) shall not process third party data for a proc-*  
24       *essing purpose other than, in the case of sensitive cov-*  
25       *ered data, the processing purpose for which the indi-*

1        *vidual gave affirmative express consent or to effect a*  
2        *purpose enumerated in paragraph (1), (3), or (5) of*  
3        *section 101(b) and, in the case of non-sensitive data,*  
4        *the processing purpose for which the covered entity*  
5        *made a disclosure pursuant to section 202(b)(4); and*  
6            *(2) for purposes of paragraph (1), may reason-*  
7        *ably rely on representations made by the covered enti-*  
8        *ty that transferred the third party data if the third*  
9        *party conducts reasonable due diligence on the rep-*  
10       *resentations of the covered entity and finds those rep-*  
11       *resentations to be credible.*

12       *(e) ADDITIONAL OBLIGATIONS ON COVERED ENTI-*  
13 *TIES.—*

14            *(1) IN GENERAL.—A covered entity or service*  
15       *provider shall exercise reasonable due diligence in—*

16            *(A) selecting a service provider; and*

17            *(B) deciding to transfer covered data to a*  
18       *third party.*

19            *(2) GUIDANCE.—Not later than 2 years after the*  
20       *date of enactment of this Act, the Commission shall*  
21       *publish guidance regarding compliance with this sub-*  
22       *section, taking into consideration the burdens on large*  
23       *data holders, covered entities who are not large data*  
24       *holders, and covered entities meeting the requirements*  
25       *of section 209.*

1           (f) *RULE OF CONSTRUCTION.*—*Solely for the purposes*  
2 *of this section, the requirements for service providers to con-*  
3 *tract with, assist, and follow the instructions of covered en-*  
4 *tities shall be read to include requirements to contract with,*  
5 *assist, and follow the instructions of a government entity*  
6 *if the service provider is providing a service to a govern-*  
7 *ment entity.*

8           **SEC. 303. TECHNICAL COMPLIANCE PROGRAMS.**

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

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

20                   (1) *establish publicly available guidelines for*  
21 *compliance with this Act; and*

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

23           (c) *APPROVAL PROCESS.*—

24                   (1) *IN GENERAL.*—*Any request for approval,*  
25 *amendment, or repeal of a technical compliance pro-*

1        *gram may be submitted to the Commission by any*  
2        *person, including a covered entity, a representative of*  
3        *a covered entity, an association of covered entities, or*  
4        *a public interest group or organization. Within 90*  
5        *days after the request is made, the Commission shall*  
6        *publish the request and provide an opportunity for*  
7        *public comment on the proposal.*

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

16       (d) *RIGHT TO APPEAL.—Final action by the Commis-*  
17       *sion on a request for approval, amendment, or repeal of*  
18       *a technical compliance program, or the failure to act within*  
19       *the 1-year period after a request for approval, amendment,*  
20       *or repeal of a technical compliance program is made under*  
21       *subsection (c), may be appealed to a Federal district court*  
22       *of the United States of appropriate jurisdiction as provided*  
23       *for in section 702 of title 5, United States Code.*

24       (e) *EFFECT ON ENFORCEMENT.—*

1           (1) *IN GENERAL.*—Prior to commencing an in-  
2           *vestigation or enforcement action against any covered*  
3           *entity under this Act, the Commission and State at-*  
4           *torney general shall consider the covered entity’s his-*  
5           *tory of compliance with any technical compliance*  
6           *program approved under this section and any action*  
7           *taken by the covered entity to remedy noncompliance*  
8           *with such program. If such enforcement action de-*  
9           *scribed in section 403 is brought, the covered entity’s*  
10          *history of compliance with any technical compliance*  
11          *program approved under this section and any action*  
12          *taken by the covered entity to remedy noncompliance*  
13          *with such program shall be taken into consideration*  
14          *when determining liability or a penalty. The covered*  
15          *entity’s history of compliance with any technical*  
16          *compliance program shall not affect any burden of*  
17          *proof or the weight given to evidence in an enforce-*  
18          *ment or judicial proceeding.*

19          (2) *COMMISSION AUTHORITY.*—Approval of a  
20          *technical compliance program shall not limit the au-*  
21          *thority of the Commission, including the Commis-*  
22          *sion’s authority to commence an investigation or en-*  
23          *forcement action against any covered entity under*  
24          *this Act or any other Act.*

1           (3) *RULE OF CONSTRUCTION.*—*Nothing in this*  
2           *subsection shall provide any individual, class of indi-*  
3           *viduals, or person with any right to seek discovery of*  
4           *any non-public Commission deliberation or activity*  
5           *or impose any pleading requirement on the Commis-*  
6           *sion if the Commission brings an enforcement action*  
7           *of any kind.*

8   **SEC. 304. COMMISSION APPROVED COMPLIANCE GUIDE-**  
9                                   **LINES.**

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

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

19               (2) *APPLICATION REQUIREMENTS.*—*Such appli-*  
20               *cation shall include—*

21                       (A) *a description of how the proposed guide-*  
22                       *lines will meet or exceed the requirements of this*  
23                       *Act;*



1           (B) a description of the entities or activities  
2           the proposed set of compliance guidelines is de-  
3           signed to cover;

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

9           (D) a description of how such covered enti-  
10          ties will be independently assessed for adherence  
11          to such compliance guidelines, including the  
12          independent organization not associated with  
13          any of the covered entities that may participate  
14          in guidelines that will administer such guide-  
15          lines.

16          (3) COMMISSION REVIEW.—

17               (A) INITIAL APPROVAL.—

18                   (i) PUBLIC COMMENT PERIOD.—Within  
19                   90 days after the receipt of proposed guide-  
20                   lines submitted pursuant to paragraph (2),  
21                   the Commission shall publish the applica-  
22                   tion and provide an opportunity for public  
23                   comment on such compliance guidelines.

24                   (ii) APPROVAL.—The Commission shall  
25                   approve an application regarding proposed

1 *guidelines under paragraph (2) if the appli-*  
2 *cant demonstrates that the compliance*  
3 *guidelines—*

4 *(I) meet or exceed requirements of*  
5 *this Act;*

6 *(II) provide for the regular review*  
7 *and validation by an independent or-*  
8 *ganization not associated with any of*  
9 *the covered entities that may partici-*  
10 *pate in the guidelines and that is ap-*  
11 *proved by the Commission to conduct*  
12 *such reviews of the compliance guide-*  
13 *lines of the covered entity or entities to*  
14 *ensure that the covered entity or enti-*  
15 *ties continue to meet or exceed the re-*  
16 *quirements of this Act; and*

17 *(III) include a means of enforce-*  
18 *ment if a covered entity does not meet*  
19 *or exceed the requirements in the*  
20 *guidelines, which may include referral*  
21 *to the Commission for enforcement con-*  
22 *sistent with section 401 or referral to*  
23 *the appropriate State attorney general*  
24 *for enforcement consistent with section*  
25 *402.*

1                   (iii) *TIMELINE.*—*Within 1 year after*  
2                   *receiving an application regarding proposed*  
3                   *guidelines under paragraph (2), the Com-*  
4                   *mission shall issue a determination approv-*  
5                   *ing or denying the application and pro-*  
6                   *viding its reasons for approving or denying*  
7                   *such application.*

8                   (B) *APPROVAL OF MODIFICATIONS.*—

9                   (i) *IN GENERAL.*—*If the independent*  
10                  *organization administering a set of guide-*  
11                  *lines makes material changes to guidelines*  
12                  *previously approved by the Commission, the*  
13                  *independent organization shall submit the*  
14                  *updated guidelines to the Commission for*  
15                  *approval. As soon as feasible, the Commis-*  
16                  *sion shall publish the updated guidelines*  
17                  *and provide an opportunity for public com-*  
18                  *ment.*

19                  (ii) *TIMELINE.*—*The Commission shall*  
20                  *approve or deny any material change to the*  
21                  *guidelines within 1 year after receipt of the*  
22                  *submission for approval.*

23                  (b) *WITHDRAWAL OF APPROVAL.*—*If at any time the*  
24                  *Commission determines that the guidelines previously ap-*  
25                  *proved no longer meet the requirements of this Act or a reg-*

1 *ulation promulgated under this Act or that compliance with*  
2 *the approved guidelines is insufficiently enforced by the*  
3 *independent organization administering the guidelines, the*  
4 *Commission shall notify the covered entities or group of*  
5 *such entities and the independent organization of the deter-*  
6 *mination of the Commission to withdraw approval of such*  
7 *guidelines and the basis for doing so. Within 180 days after*  
8 *receipt of such notice, the covered entity or group of such*  
9 *entities and the independent organization may cure any al-*  
10 *leged deficiency with the guidelines or the enforcement of*  
11 *such guidelines and submit each proposed cure to the Com-*  
12 *mission. If the Commission determines that such cures*  
13 *eliminate the alleged deficiency in the guidelines, then the*  
14 *Commission may not withdraw approval of such guidelines*  
15 *on the basis of such determination.*

16 *(c) DEEMED COMPLIANCE.—A covered entity that is*  
17 *eligible to participate under subsection (a)(1) and partici-*  
18 *pates in guidelines approved under this section shall be*  
19 *deemed in compliance with the relevant provisions of this*  
20 *Act if such covered entity is in compliance with such guide-*  
21 *lines.*

22 **SEC. 305. DIGITAL CONTENT FORGERIES.**

23 *(a) REPORTS.—Not later than 1 year after the date*  
24 *of enactment of this Act, and annually thereafter, the Sec-*

1 *retary of Commerce or the Secretary's designee shall publish*  
2 *a report regarding digital content forgeries.*

3 (b) *REQUIREMENTS.—Each report under subsection*  
4 *(a) shall include the following:*

5 (1) *A definition of digital content forgeries along*  
6 *with accompanying explanatory materials.*

7 (2) *A description of the common sources of dig-*  
8 *ital content forgeries in the United States and com-*  
9 *mercial sources of digital content forgery technologies.*

10 (3) *An assessment of the uses, applications, and*  
11 *harms of digital content forgeries.*

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

19 (5) *A description of the types of digital content*  
20 *forgeries, including those used to commit fraud, cause*  
21 *harm, or violate any provision of law.*

22 (6) *Any other information determined appro-*  
23 *priate by the Secretary of Commerce or the Sec-*  
24 *retary's designee.*

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

4 **SEC. 401. ENFORCEMENT BY THE FEDERAL TRADE COMMIS-**  
5 **SION.**

6 (a) *BUREAU OF PRIVACY.—*

7 (1) *IN GENERAL.—The Commission shall estab-*  
8 *lish within the Commission a new bureau to be*  
9 *known as the “Bureau of Privacy”, which shall be of*  
10 *similar structure, size, organization, and authority as*  
11 *the existing bureaus within the Commission related to*  
12 *consumer protection and competition.*

13 (2) *MISSION.—The mission of the Bureau estab-*  
14 *lished under paragraph (1) shall be to assist the Com-*  
15 *mission in carrying out the duties of the Commission*  
16 *under this Act and related duties under other provi-*  
17 *sions of law.*

18 (3) *TIMELINE.—The Bureau required to be estab-*  
19 *lished under paragraph (1) shall be established,*  
20 *staffed, and fully operational not later than 1 year*  
21 *after the date of enactment of this Act.*

22 (b) *OFFICE OF BUSINESS MENTORSHIP.—The Director*  
23 *of the Bureau established under subsection (a)(1) shall es-*  
24 *tablish within the Bureau an office to be known as the “Of-*  
25 *fice of Business Mentorship” to provide guidance and edu-*

1 *cation to covered entities and service providers regarding*  
2 *compliance with this Act. Covered entities or service pro-*  
3 *viders may request advice from the Commission or the Of-*  
4 *fice with respect to a course of action that the covered entity*  
5 *or service provider proposes to pursue and that may relate*  
6 *to the requirements of this Act.*

7 *(c) ENFORCEMENT BY THE FEDERAL TRADE COMMIS-*  
8 *SION.—*

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

16 *(2) POWERS OF THE COMMISSION.—*

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

1           (B) *PRIVILEGES AND IMMUNITIES.*—Any  
2           person who violates this Act or a regulation pro-  
3           mulgated under this Act shall be subject to the  
4           penalties and entitled to the privileges and im-  
5           munities provided in the Federal Trade Commis-  
6           sion Act (15 U.S.C. 41 et seq.).

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

17          (4) *COMMON CARRIERS AND NONPROFIT ORGANI-*  
18          *ZATIONS.*—Notwithstanding any jurisdictional limi-  
19          tation of the Commission with respect to consumer  
20          protection or privacy, the Commission shall enforce  
21          this Act and the regulations promulgated under this  
22          Act, in the same manner provided in paragraphs (1),  
23          (2), (3), and (5), with respect to common carriers  
24          subject to the Communications Act of 1934 (47 U.S.C.  
25          151 et seq.) and all Acts amendatory thereof and sup-



1        *plementary thereto and organizations not organized*  
2        *to carry on business for their own profit or that of*  
3        *their members.*

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

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

11           (B) *DEPOSITS.—Notwithstanding section*  
12        *3302 of title 31, United States Code, in any ju-*  
13        *dicial or administrative action to enforce this*  
14        *Act or a regulation promulgated under this Act,*  
15        *the amount of any civil penalty obtained against*  
16        *a covered entity or service provider, or any other*  
17        *monetary relief ordered to be paid by a covered*  
18        *entity or service provider to provide redress,*  
19        *payment, compensation, or other relief to indi-*  
20        *viduals that cannot be located or the payment of*  
21        *which would otherwise not be practicable, shall*  
22        *be deposited into the Victims Relief Fund.*

23           (C) *USE OF FUNDS.—*

24           (i) *USE BY COMMISSION.—Amounts in*  
25        *the Victims Relief Fund shall be available*

1           to the Commission, without fiscal year limi-  
2           tation, to provide redress, payment, com-  
3           pensation, or other monetary relief to indi-  
4           viduals affected by an act or practice for  
5           which relief has been obtained under this  
6           Act.

7           (ii) *OTHER PERMISSIBLE USES.*—To  
8           the extent that the individuals described in  
9           clause (i) cannot be located or such redress,  
10          payments, compensation, or other monetary  
11          relief are otherwise not practicable, the  
12          Commission may use such funds for the  
13          purpose of—

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

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

21 **SEC. 402. ENFORCEMENT BY STATES.**

22          (a) *CIVIL ACTION.*—In any case in which the attorney  
23          general or State Privacy Authority of a State has reason  
24          to believe that an interest of the residents of that State has  
25          been, may be, or is adversely affected by a violation of this

1 *Act or a regulation promulgated under this Act by a covered*  
2 *entity or service provider, the attorney general or State Pri-*  
3 *vacancy Authority may bring a civil action in the name of*  
4 *the State, or as parens patriae on behalf of the residents*  
5 *of the State. Any such action shall be brought exclusively*  
6 *in an appropriate Federal district court of the United*  
7 *States to—*

8 *(1) enjoin such act or practice;*

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

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

14 *(4) obtain reasonable attorneys' fees and other*  
15 *litigation costs reasonably incurred.*

16 *(b) RIGHTS OF THE COMMISSION.—*

17 *(1) IN GENERAL.—Except as provided in para-*  
18 *graph (2), the attorney general or State Privacy Au-*  
19 *thority of a State shall notify the Commission in*  
20 *writing prior to initiating a civil action under sub-*  
21 *section (a). Such notification shall include a copy of*  
22 *the complaint to be filed to initiate such action. Upon*  
23 *receiving such notification, the Commission may in-*  
24 *tervene in such action as a matter of right pursuant*  
25 *to the Federal Rules of Civil Procedure.*

1           (2) *FEASIBILITY.*—*If the notification required by*  
2           *paragraph (1) is not feasible, the attorney general or*  
3           *State Privacy Authority shall notify the Commission*  
4           *immediately after initiating the civil action.*

5           (c) *ACTIONS BY THE COMMISSION.*—*In any case in*  
6           *which a civil action is instituted by or on behalf of the Com-*  
7           *mission for violation of this Act or a regulation promul-*  
8           *gated under this Act, no attorney general or State Privacy*  
9           *Authority of a State may, during the pendency of such ac-*  
10          *tion, institute a civil action against any defendant named*  
11          *in the complaint in the action instituted by or on behalf*  
12          *of the Commission for a violation of this Act or a regulation*  
13          *promulgated under this Act that is alleged in such com-*  
14          *plaint, if such complaint alleges such violation affected the*  
15          *residents of such State or individuals nationwide. If the*  
16          *Commission brings a civil action against a covered entity*  
17          *or service provider for a violation of this Act or a regulation*  
18          *promulgated under this Act that affects the interests of the*  
19          *residents of a State, the attorney general or State Privacy*  
20          *Authority of such State may intervene in such action as*  
21          *a matter of right pursuant to the Federal Rules of Civil*  
22          *Procedure.*

23          (d) *RULE OF CONSTRUCTION.*—*Nothing in this section*  
24          *may be construed to prevent the attorney general or State*  
25          *Privacy Authority of a State from exercising the powers*

1 *conferred on the attorney general or State Privacy Author-*  
2 *ity to conduct investigations, to administer oaths or affir-*  
3 *mations, or to compel the attendance of witnesses or the*  
4 *production of documentary or other evidence.*

5 *(e) PRESERVATION OF STATE POWERS.—Except as*  
6 *provided in subsection (c), nothing in this section may be*  
7 *construed as altering, limiting, or affecting the authority*  
8 *of the attorney general or State Privacy Authority of a*  
9 *State to—*

10 *(1) bring an action or other regulatory pro-*  
11 *ceeding arising solely under the law in effect in the*  
12 *State that is preempted by this Act or under another*  
13 *applicable Federal law; or*

14 *(2) exercise the powers conferred on the attorney*  
15 *general or State Privacy Authority by the laws of the*  
16 *State, including the ability to conduct investigations,*  
17 *administer oaths or affirmations, or compel the at-*  
18 *tendance of witnesses or the production of documen-*  
19 *tary or other evidence.*

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

21 *(a) ENFORCEMENT BY PERSONS.—*

22 *(1) IN GENERAL.—Beginning on the date that is*  
23 *2 years after the date on which this Act takes effect,*  
24 *any person or class of persons for a violation of this*  
25 *Act or a regulation promulgated under this Act by a*

1        *covered entity or service provider may bring a civil*  
2        *action against such entity in any Federal court of*  
3        *competent jurisdiction.*

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

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

9            (B) *injunctive relief;*

10          (C) *declaratory relief; and*

11          (D) *reasonable attorney’s fees and litigation*  
12        *costs.*

13            (3) *RIGHTS OF THE COMMISSION AND STATE AT-*  
14        *TORNEYS GENERAL.—*

15            (A) *IN GENERAL.—Prior to a person bring-*  
16        *ing a civil action under paragraph (1), such per-*  
17        *son shall notify the Commission and the attorney*  
18        *general of the State where such person resides in*  
19        *writing that such person intends to bring a civil*  
20        *action under such paragraph. Upon receiving*  
21        *such notice, the Commission and State attorney*  
22        *general shall each or jointly make a determina-*  
23        *tion and respond to such person not later than*  
24        *60 days after receiving such notice, as to whether*  
25        *they will intervene in such action pursuant to*

1           *the Federal Rules of Civil Procedure. If a state*  
2           *attorney general does intervene, they shall only*  
3           *be heard with respect to the interests of the resi-*  
4           *dents of their State*

5                   *(B) RETAINED AUTHORITY.—Subparagraph*  
6           *(A) may not be construed to limit the authority*  
7           *of the Commission or any applicable State attor-*  
8           *ney general or State Privacy Authority to later*  
9           *commence a proceeding or civil action or inter-*  
10           *vene by motion if the Commission or State attor-*  
11           *ney general or State Privacy Authority does not*  
12           *commence a proceeding or civil action within the*  
13           *60-day period.*

14                   *(C) BAD FAITH.—Any written communica-*  
15           *tion from counsel for an aggrieved party to a*  
16           *covered entity or service provider requesting a*  
17           *monetary payment from that covered entity or*  
18           *service provider regarding a specific claim de-*  
19           *scribed in a letter sent pursuant to subsection*  
20           *(d), not including filings in court proceedings,*  
21           *arbitrations, mediations, judgment collection*  
22           *processes, or other communications related to*  
23           *previously initiated litigation or arbitrations,*  
24           *shall be considered to have been sent in bad faith*  
25           *and shall be unlawful as defined in this Act, if*

1           *the written communication was sent prior to the*  
2           *date that is 60 days after either a State attorney*  
3           *general or the Commission has received the no-*  
4           *tice required under subparagraph (A).*

5           *(4) FTC STUDY.—Beginning on the date that is*  
6           *5 years after the date of enactment of this Act and*  
7           *every 5 years thereafter, the Commission’s Bureau of*  
8           *Economics and Bureau of Privacy shall assist the*  
9           *Commission in conducting a study to determine the*  
10          *economic impacts in the United States of demand let-*  
11          *ters sent pursuant to this section and the scope of the*  
12          *rights of a person under this section to bring forth*  
13          *civil actions against covered entities and service pro-*  
14          *viders. Such study shall include the following:*

15                   *(A) The impact on insurance rates in the*  
16                   *United States.*

17                   *(B) The impact on the ability of covered en-*  
18                   *tities to offer new products or services.*

19                   *(C) The impact on the creation and growth*  
20                   *of new startup companies, including new tech-*  
21                   *nology companies.*

22                   *(D) Any emerging risks, benefits, and long-*  
23                   *term trends in relevant marketplaces, supply*  
24                   *chains, and labor availability.*



1           (E) *The impact on reducing, preventing, or*  
2           *remediating harms to individuals, including*  
3           *from fraud, identity theft, spam, discrimination,*  
4           *defective products, and violations of rights.*

5           (F) *The impact on the volume and severity*  
6           *of data security incidents, and the ability to re-*  
7           *spond to data security incidents.*

8           (G) *Other intangible direct and indirect*  
9           *costs and benefits to individuals.*

10          (5) *REPORT TO CONGRESS.—Not later than 5*  
11          *years after the first day on which persons and classes*  
12          *of persons are able to bring civil actions under this*  
13          *subsection, and annually thereafter, the Commission*  
14          *shall submit to the Committee on Energy and Com-*  
15          *merce of the House of Representatives and the Com-*  
16          *mittee on Commerce, Science, and Transportation of*  
17          *the Senate a report that contains the results of the*  
18          *study conducted under paragraph (4).*

19          (b) *ARBITRATION AGREEMENTS AND PRE-DISPUTE*  
20          *JOINT ACTION WAIVERS.—*

21                 (1) *PRE-DISPUTE ARBITRATION AGREEMENTS.—*

22                         (A) *Notwithstanding any other provision of*  
23                         *law, no pre-dispute arbitration agreement with*  
24                         *respect to an individual under the age of 18 is*

1           *enforceable with regard to a dispute arising*  
2           *under this Act.*

3           *(B) Notwithstanding any other provision of*  
4           *law, no pre-dispute arbitration agreement is en-*  
5           *forceable with regard to a dispute arising under*  
6           *this Act concerning a claim related to gender or*  
7           *partner-based violence or physical harm.*

8           *(2) PRE-DISPUTE JOINT-ACTION WAIVERS.—Not-*  
9           *withstanding any other provision of law, no pre-dis-*  
10          *pute joint-action waiver with respect to an individual*  
11          *under the age of 18 is enforceable with regard to a*  
12          *dispute arising under this Act.*

13          *(3) DEFINITIONS.—For purposes of this sub-*  
14          *section:*

15                 *(A) PRE-DISPUTE ARBITRATION AGREE-*  
16                 *MENT.—The term “pre-dispute arbitration agree-*  
17                 *ment” means any agreement to arbitrate a dis-*  
18                 *pute that has not arisen at the time of the mak-*  
19                 *ing of the agreement.*

20                 *(B) PRE-DISPUTE JOINT-ACTION WAIVER.—*  
21                 *The term “pre-dispute joint-action waiver”*  
22                 *means an agreement, whether or not part of a*  
23                 *pre-dispute arbitration agreement, that would*  
24                 *prohibit or waive the right of 1 of the parties to*  
25                 *the agreement to participate in a joint, class, or*

1           *collective action in a judicial, arbitral, adminis-*  
2           *trative, or other related forum, concerning a dis-*  
3           *pute that has not yet arisen at the time of the*  
4           *making of the agreement.*

5           *(c) RIGHT TO CURE.—*

6           *(1) NOTICE.—Subject to paragraph (3), with re-*  
7           *spect to a claim under this section for—*

8                     *(A) injunctive relief; or*

9                     *(B) an action against a covered entity or*  
10           *service provider that meets the requirements of*  
11           *section 209 of this Act, such claim may be*  
12           *brought by a person or class of persons if—prior*  
13           *to asserting such claim—the person or class or*  
14           *persons provides to the covered entity or service*  
15           *provider 45 days' written notice identifying the*  
16           *specific provisions of this Act the person or class*  
17           *of persons alleges have been or are being violated.*

18           *(2) EFFECT OF CURE.—Subject to paragraph*  
19           *(3), in the event a cure is possible, if within the 45*  
20           *days the covered entity or service provider dem-*  
21           *onstrates to the court that it has cured the noticed*  
22           *violation or violations and provides the person or*  
23           *class of persons an express written statement that the*  
24           *violation or violations has been cured and that no*  
25           *further violations shall occur, a claim for injunctive*

1       *relief shall not be permitted and may be reasonably*  
2       *dismissed.*

3               (3) *RULE OF CONSTRUCTION.*—*The notice de-*  
4       *scribed in paragraph (1) and the reasonable dismissal*  
5       *in paragraph (2) shall not apply more than once to*  
6       *any alleged underlying violation by the same covered*  
7       *entity.*

8               (d) *DEMAND LETTER.*—*If a person or a identified*  
9       *members of a class of persons represented by counsel in re-*  
10       *gard to an alleged violation or violations of the Act and*  
11       *has correspondence sent to a covered entity or service pro-*  
12       *vider by counsel alleging a violation or violations of the*  
13       *provisions of this Act and requests a monetary payment,*  
14       *such correspondence shall include the following language:*  
15       *“Please visit the website of the Federal Trade Commission*  
16       *for a general description of your rights under the American*  
17       *Data Privacy and Protection Act” followed by a hyperlink*  
18       *to the webpage of the Commission required under section*  
19       *201. If such correspondence does not include such language*  
20       *and hyperlink, a civil action brought under this section by*  
21       *such person or identified members of the class of persons*  
22       *represented by counsel may be dismissed without prejudice*  
23       *and shall not be reinstated until such person or persons has*  
24       *complied with this subsection.*

25               (e) *APPLICABILITY.*—

1           (1) *IN GENERAL.*—*This section shall only apply*  
2 *to a claim alleging a violation of section 102, 104,*  
3 *202, 203, 204, 205(a), 205(b), 206(b)(3)(C), 207(a),*  
4 *208(a), or 302, or a regulation promulgated under*  
5 *any such section.*

6           (2) *EXCEPTION.*—*This section shall not apply to*  
7 *any claim against a covered entity that has less than*  
8 *\$25,000,000 per year in revenue, collects, processes, or*  
9 *transfers the covered data of fewer than 50,000 indi-*  
10 *viduals, and derives less than 50 percent of its rev-*  
11 *enue from transferring covered data.*

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

13 (a) *FEDERAL LAW PRESERVATION.*—

14           (1) *IN GENERAL.*—*Nothing in this Act or a regu-*  
15 *lation promulgated under this Act may be construed*  
16 *to limit—*

17                   (A) *the authority of the Commission, or any*  
18 *other Executive agency, under any other provi-*  
19 *sion of law;*

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

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

1           (2) *ANTITRUST SAVINGS CLAUSE.*—

2                   (A) *FULL APPLICATION OF THE ANTITRUST*  
3 *LAW.*—*Nothing in this Act may be construed to*  
4 *modify, impair or supersede the operation of the*  
5 *antitrust law or any other provision of law.*

6                   (B) *NO IMMUNITY FROM THE ANTITRUST*  
7 *LAW.*—*Nothing in the regulatory regime adopted*  
8 *by this Act shall be construed as operating to*  
9 *limit any law deterring anticompetitive conduct*  
10 *or diminishing the need for full application of*  
11 *the antitrust law. Nothing in this Act explicitly*  
12 *or implicitly precludes the application of the*  
13 *antitrust law.*

14                  (C) *DEFINITION OF ANTITRUST LAW.*—*For*  
15 *purposes of this section, the term antitrust law*  
16 *has the same meaning as in subsection (a) of the*  
17 *first section of the Clayton Act (15 U.S.C. 12),*  
18 *except that such term includes section 5 of the*  
19 *Federal Trade Commission Act (15 U.S.C. 45) to*  
20 *the extent that such section 5 applies to unfair*  
21 *methods of competition.*

22           (3) *APPLICABILITY OF OTHER PRIVACY REQUIRE-*  
23 *MENTS.*—*A covered entity that is required to comply*  
24 *with title V of the Gramm-Leach-Bliley Act (15*  
25 *U.S.C. 6801 et seq.), the Health Information Tech-*

1        *nology for Economic and Clinical Health Act (42*  
2        *U.S.C. 17931 et seq.), part C of title XI of the Social*  
3        *Security Act (42 U.S.C. 1320d et seq.), the Fair Cred-*  
4        *it Reporting Act (15 U.S.C. 1681 et seq.), the Family*  
5        *Educational Rights and Privacy Act (20 U.S.C.*  
6        *1232g; part 99 of title 34, Code of Federal Regula-*  
7        *tions) to the extent such covered entity is a school as*  
8        *defined in 20 U.S.C. 1232g(a)(3) or 34 C.F.R.*  
9        *99.1(a), section 444 of the General Education Provi-*  
10       *sions Act (commonly known as the “Family Edu-*  
11       *cational Rights and Privacy Act of 1974”) (20 U.S.C.*  
12       *1232g) and part 99 of title 34, Code of Federal Regu-*  
13       *lations (or any successor regulation), the Confiden-*  
14       *tiality of Alcohol and Drug Abuse Patient Records at*  
15       *42 U.S.C. 290dd-2 and its implementing regulations*  
16       *at 42 CFR part 2, the Genetic Information Non-dis-*  
17       *crimination Act (GINA), or the regulations promul-*  
18       *gated pursuant to section 264(c) of the Health Insur-*  
19       *ance Portability and Accountability Act of 1996 (42*  
20       *U.S.C. 1320d–2 note), and is in compliance with the*  
21       *data privacy requirements of such regulations, part,*  
22       *title, or Act (as applicable), shall be deemed to be in*  
23       *compliance with the related requirements of this Act,*  
24       *except for section 208, solely and exclusively with re-*  
25       *spect to data subject to the requirements of such regu-*

1        *lations, part, title, or Act. Not later than 1 year after*  
2        *the date of enactment of this Act, the Commission*  
3        *shall issue guidance describing the implementation of*  
4        *this paragraph.*

5            (4) *APPLICABILITY OF OTHER DATA SECURITY*  
6        *REQUIREMENTS.—A covered entity that is required to*  
7        *comply with title V of the Gramm-Leach-Bliley Act*  
8        *(15 U.S.C. 6801 et seq.), the Health Information*  
9        *Technology for Economic and Clinical Health Act (42*  
10       *U.S.C. 17931 et seq.), part C of title XI of the Social*  
11       *Security Act (42 U.S.C. 1320d et seq.), or the regula-*  
12       *tions promulgated pursuant to section 264(c) of the*  
13       *Health Insurance Portability and Accountability Act*  
14       *of 1996 (42 U.S.C. 1320d–2 note), and is in compli-*  
15       *ance with the information security requirements of*  
16       *such regulations, part, title, or Act (as applicable),*  
17       *shall be deemed to be in compliance with the require-*  
18       *ments of section 208, solely and exclusively with re-*  
19       *spect to data subject to the requirements of such regu-*  
20       *lations, part, title, or Act. Not later than 1 year after*  
21       *the date of enactment of this Act, the Commission*  
22       *shall issue guidance describing the implementation of*  
23       *this paragraph.*

24       (b) *PREEMPTION OF STATE LAWS.—*



1           (1) *IN GENERAL.*—No State or political subdivi-  
2           sion of a State may adopt, maintain, enforce, pre-  
3           scribe, or continue in effect any law, regulation, rule,  
4           standard, requirement, or other provision having the  
5           force and effect of law of any State, or political sub-  
6           division of a State, covered by the provisions of this  
7           Act, or a rule, regulation, or requirement promul-  
8           gated under this Act.

9           (2) *STATE LAW PRESERVATION.*—Paragraph (1)  
10          may not be construed to preempt, displace, or sup-  
11          plant the following State laws, rules, regulations, or  
12          requirements:

13                (A) *Consumer protection laws of general ap-*  
14                *plicability, such as laws regulating deceptive,*  
15                *unfair, or unconscionable practices, except that*  
16                *the fact of a violation of this Act or a regulation*  
17                *promulgated under this Act may not be pleaded*  
18                *as an element of any violation of such a law.*

19                (B) *Civil rights laws.*

20                (C) *Provisions of laws, in so far as, that*  
21                *govern the privacy rights or other protections of*  
22                *employees, employee information, students, or*  
23                *student information.*

24                (D) *Laws that address notification require-*  
25                *ments in the event of a data breach.*

1                   (E) *Contract or tort law.*

2                   (F) *Criminal laws.*

3                   (G) *Civil laws governing fraud, theft (in-*  
4 *cluding identity theft), unauthorized access to in-*  
5 *formation or electronic devices, unauthorized use*  
6 *of information, malicious behavior, or similar*  
7 *provisions of law.*

8                   (H) *Civil laws regarding cyberstalking,*  
9 *cyberbullying, nonconsensual pornography, sex-*  
10 *ual harassment, child abuse material, child por-*  
11 *nography, child abduction or attempted child ab-*  
12 *duction, coercion or enticement of a child for sex-*  
13 *ual activity, or child sex trafficking.*

14                  (I) *Public safety or sector specific laws un-*  
15 *related to privacy or security.*

16                  (J) *Provisions of law, insofar as such provi-*  
17 *sions address public records, criminal justice in-*  
18 *formation systems, arrest records, mug shots,*  
19 *conviction records, or non-conviction records.*

20                  (K) *Provisions of law, insofar as such pro-*  
21 *visions address banking records, financial*  
22 *records, tax records, Social Security numbers,*  
23 *credit cards, consumer and credit reporting and*  
24 *investigations, credit repair, credit clinics, or*  
25 *check-cashing services.*

1           (L) Provisions of law, insofar as such provi-  
2           sions address facial recognition or facial recogni-  
3           tion technologies, electronic surveillance, wire-  
4           tapping, or telephone monitoring.

5           (M) The Biometric Information Privacy Act  
6           (740 ICLS 14 et seq.) and the Genetic Informa-  
7           tion Privacy Act (410 ILCS 513 et seq.).

8           (N) Provisions of laws, in so far as, such  
9           provisions to address unsolicited email or text  
10          messages, telephone solicitation, or caller identi-  
11          fication.

12          (O) Provisions of laws, in so far as, such  
13          provisions address health information, medical  
14          information, medical records, HIV status, or  
15          HIV testing.

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

19          (Q) Provisions of law, insofar as such pro-  
20          visions address the confidentiality of library  
21          records.

22          (R) Section 1798.150 of the California Civil  
23          Code (as amended on November 3, 2020 by ini-  
24          tiative Proposition 24, Section 16).

1           (8) *Laws pertaining to the use of*  
2           *encryption as a means of providing data secu-*  
3           *rity.*

4           (3) *CPPA ENFORCEMENT.—Notwithstanding*  
5           *any other provisions of law, the California Privacy*  
6           *Protection Agency established under 1798.199.10(a) of*  
7           *the California Privacy Rights Act may enforce this*  
8           *Act, in the same manner, it would otherwise enforce*  
9           *the California Consumer Privacy Act, Section*  
10          *1798.1050 et. seq.*

11          (4) *NONAPPLICATION OF FCC PRIVACY LAWS AND*  
12          *REGULATIONS TO CERTAIN COVERED ENTITIES.—Not-*  
13          *withstanding any other provision of law, sections 222,*  
14          *338(i), and 631 of the Communications Act of 1934*  
15          *(47 U.S.C. 222; 338(i); 551), and any regulations*  
16          *and orders promulgated by the Federal Communica-*  
17          *tions Commission under any such section, do not*  
18          *apply to any covered entity with respect to the collec-*  
19          *tion, processing, transfer, or security of covered data*  
20          *or its equivalent, and the related privacy and data se-*  
21          *curity activities of a covered entity that would other-*  
22          *wise be regulated under such sections shall be gov-*  
23          *erned exclusively by the provisions of this Act, except*  
24          *for—*

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

4           (B) subsections (b) and (g) of section 222 of  
5           the Communications Act of 1934 (47 U.S.C.  
6           222); and

7           (C) any obligation of an international trea-  
8           ty related to the exchange of traffic implemented  
9           and enforced by the Federal Communications  
10          Commission.

11          (c) *PRESERVATION OF COMMON LAW OR STATUTORY*  
12          *CAUSES OF ACTION FOR CIVIL RELIEF.*—Nothing in this  
13          Act, nor any amendment, standard, rule, requirement, as-  
14          sessment, or regulation promulgated under this Act, may  
15          be construed to preempt, displace, or supplant any Federal  
16          or State common law rights or remedies, or any statute cre-  
17          ating a remedy for civil relief, including any cause of action  
18          for personal injury, wrongful death, property damage, or  
19          other financial, physical, reputational, or psychological in-  
20          jury based in negligence, strict liability, products liability,  
21          failure to warn, an objectively offensive intrusion into the  
22          private affairs or concerns of the individual, or any other  
23          legal theory of liability under any Federal or State common  
24          law, or any State statutory law.

1 **SEC. 405. SEVERABILITY.**

2 *If any provision of this Act, or the application thereof*  
3 *to any person or circumstance, is held invalid, the remain-*  
4 *der of this Act, and the application of such provision to*  
5 *other persons not similarly situated or to other cir-*  
6 *cumstances, shall not be affected by the invalidation.*

7 **SEC. 406. COPPA.**

8 *(a) IN GENERAL.—Nothing in this Act may be con-*  
9 *strued to relieve or change any obligation that a covered*  
10 *entity or other person may have under the Children’s On-*  
11 *line Privacy Protection Act of 1998 (15 U.S.C. 6501 et*  
12 *seq.).*

13 *(b) UPDATED REGULATIONS.—Not later than 180 days*  
14 *after the date of enactment of this Act, the Commission shall*  
15 *amend its rules issued pursuant to the regulations promul-*  
16 *gated by the Commission under the Children’s Online Pri-*  
17 *vacy Protection Act of 1998 (15 U.S.C. 6501 et seq.) to*  
18 *make reference to the additional requirements placed on*  
19 *covered entities under this Act, in addition to the require-*  
20 *ments under the Children’s Online Privacy Protection Act*  
21 *of 1998 that may already apply to certain covered entities.*

22 **SEC. 407. AUTHORIZATION OF APPROPRIATIONS.**

23 *There are authorized to be appropriated to the Com-*  
24 *mission such sums as may be necessary to carry out this*  
25 *Act.*

1 **SEC. 408. EFFECTIVE DATE.**

2 *This Act shall take effect on the date that is 180 days*

3 *after the date of enactment of this Act.*