

118TH CONGRESS  
2D SESSION

**S.** \_\_\_\_\_

To establish protections for covered data of individuals, and for other purposes.

---

IN THE SENATE OF THE UNITED STATES

---

\_\_\_\_\_ introduced the following bill; which was read twice and referred to the Committee on \_\_\_\_\_

---

**A BILL**

To establish protections for covered data of individuals, and for other purposes.

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

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

4 (a) SHORT TITLE.—This Act may be cited as the [“  
5 \_\_\_\_\_ Act of \_\_\_\_\_”].

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

- Sec. 1. Short title; table of contents.
- Sec. 2. Definitions.
- Sec. 3. Data minimization.
- Sec. 4. Transparency.
- Sec. 5. Individual control over covered data.
- Sec. 6. Opt-out rights and centralized mechanism.
- Sec. 7. Interference with consumer rights.

- Sec. 8. Prohibition on denial of service and waiver of rights.
- Sec. 9. Data security and protection of covered data.
- Sec. 10. Executive responsibility.
- Sec. 11. Service providers and third parties.
- Sec. 12. Data brokers.
- Sec. 13. Civil rights and algorithms.
- Sec. 14. Consequential decision opt out.
- Sec. 15. Commission approved compliance guidelines.
- Sec. 16. Privacy-enhancing technology pilot program.
- Sec. 17. Enforcement by the Federal Trade Commission.
- Sec. 18. Enforcement by States.
- Sec. 19. Enforcement by individuals.
- Sec. 20. Relation to other laws.
- Sec. 21. Children’s Online Privacy Protection Act of 1998.
- Sec. 22. Termination of FTC rulemaking on commercial surveillance and data security.
- Sec. 23. Severability.
- Sec. 24. Effective date.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

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

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

7 (i) clearly communicates the individ-  
8 ual’s authorization for an act or practice;

9 (ii) is in response to a specific request  
10 from a covered entity, or service provider  
11 on behalf of a covered entity; and

12 (iii) meets the requirements of sub-  
13 paragraph (B).

14 (B) **REQUEST REQUIREMENTS.**—The re-  
15 quirements of this subparagraph, with respect  
16 to a request made under subparagraph (A), are  
17 the following:

1 (i) The request is provided to the indi-  
2 vidual in a clear and conspicuous stand-  
3 alone disclosure.

4 (ii) The request includes a description  
5 of each act or practice for which the indi-  
6 vidual's consent is sought and—

7 (I) clearly distinguishes between  
8 an act or practice which is necessary  
9 to fulfill a request of the individual  
10 and an act or practice which is for an-  
11 other purpose;

12 (II) clearly states the specific  
13 categories of covered data that the  
14 covered entity shall collect, process,  
15 retain, or transfer to fulfill the re-  
16 quest; and

17 (III) is written in easy-to-under-  
18 stand language and includes a promi-  
19 nent heading that would enable a rea-  
20 sonable individual to identify and un-  
21 derstand the act or practice.

22 (iii) The request clearly explains the  
23 individual's applicable rights related to  
24 consent.

1 (iv) The request is made in a manner  
2 reasonably accessible to and usable by indi-  
3 viduals with disabilities.

4 (v) The request is made available to  
5 the individual in each language in which  
6 the covered entity provides a product or  
7 service for which authorization is sought.

8 (vi) The option to refuse consent shall  
9 be at least as prominent as the option to  
10 accept, and the option to refuse consent  
11 shall take the same number of steps or  
12 fewer as the option to accept.

13 (C) EXPRESS CONSENT REQUIRED.—Af-  
14 firmative express consent to an act or practice  
15 shall not be inferred from the inaction of the in-  
16 dividual or the individual's continued use of a  
17 service or product provided by the covered enti-  
18 ty.

19 (2) BIOMETRIC INFORMATION.—

20 (A) IN GENERAL.—The term “biometric  
21 information” means any covered data that is  
22 specific to an individual and is generated from  
23 the measurement or processing of the individ-  
24 ual's unique biological, physical, or physiological

1 characteristics that is linked or reasonably  
2 linkable to the individual, including—

- 3 (i) fingerprints;  
4 (ii) voice prints;  
5 (iii) iris or retina imagery scans;  
6 (iv) facial or hand mapping, geometry,  
7 templates; or  
8 (v) gait.

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

- 11 (i) a digital or physical photograph;  
12 (ii) an audio or video recording; or  
13 (iii) metadata associated with a digital  
14 or physical photograph or an audio or  
15 video recording that cannot be used to  
16 identify an individual.

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

21 (4) COMMISSION.—The term “Commission”  
22 means the Federal Trade Commission.

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

1           (6) CONNECTED DEVICE.—The term “con-  
2           nected device” means a device that is capable of con-  
3           necting to the internet over a fixed or wireless con-  
4           nection.

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

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

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

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

15           (8) COVERED ALGORITHM.—The term “covered  
16           algorithm” means a computational process, includ-  
17           ing one derived from machine learning, statistics, or  
18           other data processing or artificial intelligence tech-  
19           niques, that makes a decision or facilitates human  
20           decision-making by using covered data, which in-  
21           cludes determining the provision of products or serv-  
22           ices or ranking, ordering, promoting, recommending,  
23           amplifying, or similarly determining the delivery or  
24           display of information to an individual.

25           (9) COVERED DATA.—

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

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

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

16                   (I) do not reveal information  
17 about an individual that meets the  
18 definition of sensitive covered data  
19 with respect to an individual; and

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

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

1 (I) a collection that is open to  
2 the public or routinely made available  
3 to researchers who are not affiliated  
4 with the library, archive, or museum;

5 (II) a public service mission;

6 (III) trained staff or volunteers  
7 to provide professional services nor-  
8 mally associated with libraries, ar-  
9 chives, or museums; and

10 (IV) collections composed of law-  
11 fully acquired materials and all licens-  
12 ing conditions for such materials are  
13 met.

14 (10) COVERED ENTITY.—

15 (A) IN GENERAL.—The term “covered en-  
16 tity”—

17 (i) means any entity that, alone or  
18 jointly with others, determines the pur-  
19 poses and means of collecting, processing,  
20 retaining, or transferring covered data  
21 and—

22 (I) is subject to the Federal  
23 Trade Commission Act (15 U.S.C. 41  
24 et seq.);



1 (II) is a common carrier subject  
2 to title II of the Communications Act  
3 of 1934 (47 U.S.C. 201–231) as cur-  
4 rently enacted or subsequently amend-  
5 ed; or

6 (III) is an organization not orga-  
7 nized to carry on business for their  
8 own profit or that of their members;

9 (ii) includes any entity that controls,  
10 is controlled by, is under common control  
11 with, or shares common branding with an-  
12 other covered entity; and

13 (iii) does not include—

14 (I) a Federal, State, Tribal, terri-  
15 torial, or local government entity such  
16 as a body, authority, board, bureau,  
17 commission, district, agency, or polit-  
18 ical subdivision of the Federal Gov-  
19 ernment or a State, Tribal, territorial,  
20 or local government;

21 (II) an entity that is collecting,  
22 processing, retaining, or transferring  
23 covered data on behalf of a Federal,  
24 State, Tribal, territorial, or local gov-  
25 ernment entity, to the extent that

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

3 (III) a small business;

4 (IV) the National Center for  
5 Missing and Exploited Children; or

6 (V) except with respect to the ob-  
7 ligations under section 9, a nonprofit  
8 organization whose primary mission is  
9 to prevent, investigate, or deter fraud  
10 or to train anti-fraud professionals or  
11 educate the public about fraud, in-  
12 cluding insurance fraud, securities  
13 fraud, and financial fraud to the ex-  
14 tent the organization collects, proc-  
15 esses, retains, or transfers covered  
16 data in furtherance of such primary  
17 mission.

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

23 (11) COVERED HIGH-IMPACT SOCIAL MEDIA  
24 COMPANY.—The term “covered high-impact social

1 media company” means a covered entity that pro-  
2 vides any internet-accessible platform where—

3 (A) such covered entity generates  
4 \$3,000,000,000 or more in global annual rev-  
5 enue, including the revenue generated by any  
6 affiliate of such covered entity;

7 (B) such platform has 300,000,000 or  
8 more global monthly active users for not fewer  
9 than 3 of the preceding 12 months on the plat-  
10 form of such covered entity; and

11 (C) such platform constitutes an online  
12 product or service that is primarily used by in-  
13 dividuals to access or share user-generated con-  
14 tent.

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

17 (13) DATA BROKER.—

18 (A) IN GENERAL.—The term “data  
19 broker” means a covered entity whose principal  
20 source of revenue is derived from processing or  
21 transferring covered data that the covered enti-  
22 ty did not collect directly from the individuals  
23 linked or linkable to such covered data.

24 (B) PRINCIPAL SOURCE OF REVENUE DE-  
25 FINED.—For purposes of this paragraph, the

1 term “principal source of revenue” means, with  
2 respect to the preceding 12-month period—

3 (i) revenue that constitutes greater  
4 than 50 percent of all revenue of the cov-  
5 ered entity during such period; or

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

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

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

20 (15) DE-IDENTIFIED DATA.—The term “de-  
21 identified data” means—

22 (A) information that cannot reasonably be  
23 used to infer or derive the identity of an indi-  
24 vidual, does not identify and is not linked or  
25 reasonably linkable to an individual or a device



1 (I) comply with all of the provi-  
2 sions of this paragraph with respect  
3 to the information; and

4 (II) require that such contractual  
5 obligations be included in all subse-  
6 quent instances for which the data  
7 may be received; or

8 (B) health information (as defined in sec-  
9 tion 262 of the Health Insurance Portability  
10 and Accountability Act of 1996 (42 U.S.C.  
11 1320d)) that has been de-identified in accord-  
12 ance with section 164.514(b) of title 45, Code  
13 of Federal Regulations, provided that if such  
14 information is subsequently provided to an enti-  
15 ty that is not an entity subject to parts 160 and  
16 164 of such title 45, such entity must comply  
17 with clauses (ii) and (iii) of subparagraph (A)  
18 for the information to be considered de-identi-  
19 fied under this Act.

20 (16) DERIVED DATA.—The term “derived data”  
21 means covered data that is created by the derivation  
22 of information, data, assumptions, correlations, in-  
23 ferences, predictions, or conclusions from facts, evi-  
24 dence, or another source of information or data  
25 about an individual or an individual’s device.

1           (17) DEVICE.—The term “device” means any  
2           electronic equipment capable of collecting, proc-  
3           essing, retaining, or transferring covered data that is  
4           used by one or more individuals, including a con-  
5           nected device or a portable connected device.

6           (18) EMPLOYEE.—The term “employee” means  
7           an individual who is an employee, director, officer,  
8           staff member, or individual working as an inde-  
9           pendent contractor that is not a service provider,  
10          volunteer, or intern of an employer, regardless of  
11          whether such individual is paid, unpaid, or employed  
12          on a temporary basis.

13          (19) EMPLOYEE INFORMATION.—The term  
14          “employee information” means covered data, biomet-  
15          ric information, or genetic information that is col-  
16          lected by a covered entity (or a service provider act-  
17          ing on behalf of a covered entity)—

18                 (A) about an individual in the course of  
19                 the individual’s employment or application for  
20                 employment (including on a contract or tem-  
21                 porary basis), provided that such data is re-  
22                 tained or processed by the covered entity or the  
23                 service provider solely for purposes necessary  
24                 for the individual’s employment or application  
25                 for employment;

1 (B) that is emergency contact information  
2 for an individual who is an employee or job ap-  
3 plicant of the covered entity, provided that such  
4 data is retained or processed by the covered en-  
5 tity or the service provider solely for the pur-  
6 pose of having an emergency contact for such  
7 individual on file; or

8 (C) about an individual (or a relative of an  
9 individual) who is an employee or former em-  
10 ployee of the covered entity for the purpose of  
11 administering benefits to which such individual  
12 or relative is entitled on the basis of the individ-  
13 ual's employment with the covered entity, pro-  
14 vided that such data is retained or processed by  
15 the covered entity or the service provider solely  
16 for the purpose of administering such benefits.

17 (20) ENTITY.—The term “entity” means an in-  
18 dividual, trust, partnership, association, organiza-  
19 tion, company, or corporation.

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

23 (22) GENETIC INFORMATION.—The term “ge-  
24 netic information” means any covered data, regard-  
25 less of its format, that concerns an identified or



1 identifiable individual’s genetic characteristics, in-  
2 cluding—

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

7 (B) genotypic and phenotypic information  
8 that results from analyzing raw sequence data  
9 described in subparagraph (A).

10 (23) HEALTH INFORMATION.—The term  
11 “health information” means information that de-  
12 scribes or reveals the past, present, or future phys-  
13 ical health, mental health, disability, diagnosis, or  
14 health condition or treatment of an individual, in-  
15 cluding the precise geolocation information of such  
16 treatment.

17 (24) INDIVIDUAL.—The term “individual”  
18 means a natural person residing in the United  
19 States.

20 (25) LARGE DATA HOLDER.—

21 (A) IN GENERAL.—The term “large data  
22 holder” means a covered entity or service pro-  
23 vider that, in the most recent calendar year had  
24 an annual gross revenue of not less than  
25 \$250,000,000 and, subject to subparagraph

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

3 (i) the covered data of—

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

6 (II) 15,000,000 portable con-  
7 nected devices that identify or are  
8 linked or reasonably linkable to 1 or  
9 more individuals; and

10 (III) 35,000,000 connected de-  
11 vices that identify or are linked or  
12 reasonable linkable to 1 or more indi-  
13 viduals; or

14 (ii) the sensitive covered data of—

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

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

21 (III) 700,000 connected devices  
22 that identify or are linked or reason-  
23 ably linkable to 1 or more individuals.

24 (B) EXCLUSIONS.—For purposes of sub-  
25 paragraph (A), a covered entity or service pro-

1 vider shall not be considered a large data holder  
2 solely on account of collecting, processing, re-  
3 taining, or transferring to a service provider—

4 (i) personal mailing or email address-  
5 es;

6 (ii) personal telephone numbers;

7 (iii) log-in information of an indi-  
8 vidual or device to allow the individual or  
9 device to log in to an account administered  
10 by the covered entity; or

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

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

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

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

9 (26) MARKET RESEARCH.—The term “market  
10 research” means the collection, processing, retention,  
11 or transfer of covered data with affirmative express  
12 consent, as reasonably necessary and proportionate  
13 to measure and analyze the market or market trends  
14 of products, services, advertising, or ideas, where the  
15 covered data is not—

16 (A) integrated into any product or service;

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

19 (C) used for targeted advertising or to oth-  
20 erwise market to any individual or individual’s  
21 device.

22 (27) MATERIAL CHANGE.—The term “material  
23 change” means, with respect to treatment of covered  
24 data, a change by an entity that would likely affect  
25 an individual’s decision to provide affirmative ex-

1 press consent for, or opt out of, the entity’s collec-  
2 tion, processing, retention, or transfer of covered  
3 data pertaining to such individual.

4 (28) ON-DEVICE DATA.—The term “on-device  
5 data” means data stored under the sole control of  
6 an individual, including on an individual’s device,  
7 and only to the extent such data is not processed or  
8 transferred by a covered entity or service provider.

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

15 (30) PRECISE GEOLOCATION INFORMATION.—  
16 The term “precise geolocation information” means  
17 information that reveals the past or present physical  
18 location of an individual or device with sufficient  
19 precision to identify—

20 (A) street-level location information of  
21 such individual or device; or

22 (B) the location of such individual or de-  
23 vice within a range of 1,850 feet or less.

24 (31) PROCESS.—The term “process” means  
25 any operation or set of operations performed on cov-

1       ered data, including analyzing, organizing, struc-  
2       turing, using, modifying, or otherwise handling cov-  
3       ered data.

4           (32) PUBLICLY AVAILABLE INFORMATION.—

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

10           (i) Federal, State, or local government  
11       records provided that the covered entity  
12       collects, processes, retains, and transfers  
13       such information in accordance with any  
14       restrictions or terms of use placed on the  
15       information by the relevant government en-  
16       tity;

17           (ii) widely distributed media;

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

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

1 (B) CLARIFICATIONS; LIMITATIONS.—

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

9 (ii) BUSINESS CONTACT INFORMA-  
10 TION.—The term “publicly available infor-  
11 mation” includes the business contact in-  
12 formation of an employee that is made  
13 available to all members of the public on a  
14 website or online service, including the em-  
15 ployee’s name, position or title, business  
16 telephone number, business email address,  
17 or address.

18 (iii) OTHER LIMITATIONS.—The term  
19 “publicly available information” does not  
20 include any of the following:

21 (I) Any obscene visual depiction  
22 (as defined for purposes of section  
23 1460 of title 18, United States Code).

24 (II) Derived data from publicly  
25 available information that reveals in-

1 formation about an individual that  
2 meets the definition of sensitive cov-  
3 ered data.

4 (III) Biometric information.

5 (IV) Genetic information.

6 (V) Covered data that has been  
7 combined with publicly available infor-  
8 mation.

9 (VI) Intimate images, authentic  
10 or generated by a computer or by arti-  
11 ficial intelligence, known to be non-  
12 consensual.

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

16 (34) SENSITIVE COVERED DATA.—

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

20 (i) A government-issued identifier,  
21 such as a social security number, passport  
22 number, or driver’s license number, that is  
23 not required by law to be displayed in pub-  
24 lic.



1 (ii) Any information that describes or  
2 reveals the past, present, or future physical  
3 health, mental health, disability, diagnosis,  
4 or healthcare condition or treatment of an  
5 individual.

6 (iii) Genetic Information.

7 (iv) A financial account number, debit  
8 card number, credit card number, or any  
9 required security or access code, password,  
10 or credentials allowing access to any such  
11 account or card.

12 (v) Biometric information.

13 (vi) Precise geolocation information.

14 (vii) An individual's private commu-  
15 nications, such as voicemails, emails, texts,  
16 direct messages, or mail, or information  
17 identifying the parties to such communica-  
18 tions, information contained in telephone  
19 bills, voice communications, and any infor-  
20 mation that pertains to the transmission of  
21 voice communications, including numbers  
22 called, numbers from which calls were  
23 placed, the time calls were made, call dura-  
24 tion, and location information of the par-  
25 ties to the call, unless the covered entity is

1 an intended recipient of the communica-  
2 tion.

3 (viii) Account or device log-in creden-  
4 tials.

5 (ix) Information revealing the sexual  
6 behavior of an individual in a manner in-  
7 consistent with the individual's reasonable  
8 expectation regarding disclosure of such in-  
9 formation.

10 (x) Calendar information, address  
11 book information, phone or text logs,  
12 photos, audio recordings, or videos in-  
13 tended for private use.

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

18 (xii) Information revealing the extent  
19 or content of any individual's access, view-  
20 ing, or other use of any video program-  
21 ming described in section 713(b)(2) of the  
22 Communications Act of 1934 (47 U.S.C.  
23 613(h)(2)), including by a provider of  
24 broadcast television service, cable service,  
25 satellite service, or streaming media serv-

1 ice, but only with regard to the transfer of  
2 such information to a third party (exclud-  
3 ing any such data used solely for transfers  
4 for independent video measurement).

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

12 (xiv) Information revealing an individ-  
13 ual's race, ethnicity, national origin, reli-  
14 gion, or sex in a manner inconsistent with  
15 the individual's reasonable expectation re-  
16 garding disclosure of such information.

17 (xv) Information revealing an individ-  
18 ual's online activities over time and across  
19 websites or online services that do not  
20 share common branding or over time on  
21 any website or online service operated by a  
22 covered high-impact social media company.

23 (xvi) Information about an individual  
24 who is a covered minor.

1                   (xvii) Any other covered data col-  
2                   lected, processed, retained, or transferred  
3                   for the purpose of identifying the data  
4                   types described in clauses (i) through (xvi).

5                   (xviii) Any other covered data, except  
6                   for expanding the categories described in  
7                   clause (ii), that the Commission determines  
8                   to be sensitive covered data through a rule-  
9                   making pursuant to section 553 of title 5,  
10                  United States Code.

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

14                         (i) is related by common ownership or  
15                         corporate control to the provider of broad-  
16                         cast television service, cable service, sat-  
17                         ellite service, or streaming media service;  
18                         and

19                         (ii) provides video programming as de-  
20                         scribed in subparagraph (A)(xii).

21                  (35) SERVICE PROVIDER.—

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

1           tions on behalf of, and at the direction of, a  
2           covered entity.

3                   (B) RULE OF CONSTRUCTION.—

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

12                  (ii) CONTEXT REQUIRED.—Whether  
13                  an entity is a “covered entity” or a “serv-  
14                  ice provider” depends on the facts sur-  
15                  rounding, and the context in which, the  
16                  data is collected, processed, retained, or  
17                  transferred.

18                  (36) SMALL BUSINESS.—

19                  (A) IN GENERAL.—The term “small busi-  
20                  ness” means an entity (including any affiliate  
21                  of the entity)—

22                   (i) whose average annual gross reve-  
23                   nues for the period of the 3 preceding cal-  
24                   endar years (or for the period during  
25                   which the covered entity has been in exist-

1                   ence if such period is less than 3 years)  
2                   did not exceed \$40,000,000;

3                   (ii) that, on average, did not annually  
4                   collect, process, retain, or transfer the cov-  
5                   ered data of more than 200,000 individuals  
6                   for any purpose other than initiating, ren-  
7                   dering, billing for, finalizing, completing,  
8                   or otherwise collecting payment for a re-  
9                   quested service or product, so long as all  
10                  covered data for such purpose was deleted  
11                  or de-identified within 90 days, except  
12                  when necessary to investigate fraud or as  
13                  consistent with a covered entity's return or  
14                  warranty policy; and

15                  (iii) that did not transfer covered data  
16                  to a third party in exchange for revenue or  
17                  anything of value.

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

1 grants, dues or other assessments, income from  
2 investments, or proceeds from the sale of real  
3 or personal property.

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

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

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

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

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

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

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

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

5                   (A) means displaying or presenting to an  
6                   individual or device identified by a unique per-  
7                   sistent identifier (or group of individuals or de-  
8                   vices identified by unique persistent identifiers)  
9                   an online advertisement that is selected based  
10                  on known or predicted preferences or interests  
11                  associated with the individual or device identi-  
12                  fied by a unique identifier; and

13                  (B) does not include—

14                   (i) advertising or marketing content to  
15                   an individual in response to the individ-  
16                   ual’s specific request for information or  
17                   feedback;

18                   (ii) first-party advertising based on an  
19                   individual’s visit to or use of a website or  
20                   online service that offers a product or serv-  
21                   ice that is related to the subject of the ad-  
22                   vertisement;

23                   (iii) contextual advertising when an  
24                   advertisement is displayed online based on



1 the content of the webpage or online serv-  
2 ice on which the advertisement appears; or  
3 (iv) processing covered data solely for  
4 measuring or reporting advertising, mar-  
5 keting, or media performance, reach, or  
6 frequency, including by independent enti-  
7 ties.

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

9 (A) means any entity that—

10 (i) receives covered data from another  
11 entity; and

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

14 (B) does not include an entity that collects  
15 covered data from another entity if the 2 enti-  
16 ties are related by common ownership or cor-  
17 porate control and share common branding.

18 (41) THIRD-PARTY DATA.—The term “third  
19 party data” means covered data that has been trans-  
20 ferred to a third party.

21 (42) TRANSFER.—The term “transfer” means  
22 to disclose, release, share, disseminate, make avail-  
23 able, sell, rent, or license covered data, orally, in  
24 writing, electronically, or by any other means for

1 consideration of any kind or for a commercial pur-  
2 pose.

3 (43) UNIQUE PERSISTENT IDENTIFIER.—The  
4 term “unique persistent identifier” means—

5 (A) a technologically created identifier to  
6 the extent that such identifier is reasonably  
7 linkable to an individual or device that identi-  
8 fies or is linked or reasonably linkable to 1 or  
9 more individuals, including a device identifier,  
10 an Internet Protocol address, cookies, beacons,  
11 pixel tags, mobile ad identifiers, or similar tech-  
12 nology, customer number, unique pseudonym,  
13 or user alias, telephone numbers, or other forms  
14 of persistent or probabilistic identifiers that are  
15 linked or reasonably linkable to 1 or more indi-  
16 viduals or devices; and

17 (B) does not include an identifier assigned  
18 by a covered entity for the specific purpose of  
19 giving effect to an individual’s exercise of af-  
20 firmative express consent or opt-out of the col-  
21 lection, processing, retaining, or transfer of cov-  
22 ered data or otherwise limiting the collection,  
23 processing, retaining, or transfer of such infor-  
24 mation.

1           (44) WIDELY DISTRIBUTED MEDIA.—The term  
2           “widely distributed media”—

3           (A) means information that is available to  
4           the general public, including information from a  
5           telephone book or online directory, a television,  
6           internet, or radio program, the news media, or  
7           an internet site that is available to the general  
8           public on an unrestricted basis; and

9           (B) does not include an obscene visual de-  
10          piction (as defined in section 1460 of title 18,  
11          United States Code).

12 **SEC. 3. DATA MINIMIZATION.**

13          (a) IN GENERAL.—Subject to subsections (b) and (c),  
14 a covered entity, or a service provider acting on behalf of  
15 a covered entity, shall not collect, process, retain, or trans-  
16 fer covered data—

17          (1) beyond what is necessary, proportionate,  
18          and limited to provide or maintain—

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

1 (B) a communication by the covered entity  
2 to the individual reasonably anticipated within  
3 the context of the relationship; or

4 (2) for a purpose other than those expressly  
5 permitted under subsection (d).

6 (b) SENSITIVE COVERED DATA.—

7 (1) IN GENERAL.—Except as expressly provided  
8 under subsection (d), a covered entity, or a service  
9 provider acting on behalf of a covered entity, shall  
10 not transfer sensitive covered data to a third party  
11 without the affirmative express consent of the indi-  
12 vidual to whom such data pertains.

13 (2) WITHDRAWAL OF AFFIRMATIVE EXPRESS  
14 CONSENT.—

15 (A) IN GENERAL.—A covered entity shall  
16 provide an individual with a means to withdraw  
17 affirmative express consent previously provided  
18 by the individual with respect to the transfer of  
19 the sensitive covered data of the individual.

20 (B) REQUIREMENTS.—The means to with-  
21 draw affirmative express consent described in  
22 subparagraph (A) shall be—

23 (i) clear and conspicuous; and

24 (ii) as easy for a reasonable individual  
25 to use as the mechanism by which the indi-

1                   vidual provided affirmative express con-  
2                   sent.

3           (c) ADDITIONAL PROTECTIONS FOR BIOMETRIC IN-  
4 FORMATION AND GENETIC INFORMATION.—

5           (1) IN GENERAL.—A covered entity, or a serv-  
6           ice provider acting on behalf of a covered entity,  
7           shall not collect, process, or retain biometric infor-  
8           mation or genetic information without the affirma-  
9           tive express consent of the individual to whom such  
10          information pertains, unless such collection, proc-  
11          essing, or retention is essential for a purpose ex-  
12          pressly permitted under paragraphs (1) through (4)  
13          or paragraphs (9) through (13) of subsection (d).

14          (2) RETENTION.—A covered entity, or service  
15          provider acting on behalf of a covered entity, shall  
16          not retain biometric or genetic information beyond  
17          the point for which a purpose that an individual pro-  
18          vided affirmative express consent under paragraph  
19          (1) has been satisfied or within 3 years of the indi-  
20          vidual's last interaction with the covered entity or  
21          service provider, whichever occurs first, unless such  
22          retention is essential for a purpose expressly per-  
23          mitted under paragraphs (1) through (4) or para-  
24          graphs (9) through (13) of subsection (d).

1           (3) TRANSFER.—A covered entity, or service  
2 provider acting on behalf of a covered entity, shall  
3 not transfer biometric information or genetic infor-  
4 mation to a third party without the affirmative ex-  
5 press consent of the individual to whom such infor-  
6 mation pertains, unless such transfer is essential for  
7 a purpose expressly permitted under paragraphs (2),  
8 (3), (4), (8), (9), (11), or (12) of subsection (d).

9           (4) WITHDRAWAL OF AFFIRMATIVE EXPRESS  
10 CONSENT.—

11           (A) IN GENERAL.—A covered entity shall  
12 provide an individual with a means to withdraw  
13 affirmative express consent previously provided  
14 by the individual with respect to the biometric  
15 information or genetic information of the indi-  
16 vidual.

17           (B) REQUIREMENTS.—The means to with-  
18 draw affirmative express consent described in  
19 subparagraph (A) shall be—

- 20                   (i) clear and conspicuous; and  
21                   (ii) as easy for a reasonable individual  
22 to use as the mechanism by which the indi-  
23 vidual provided affirmative express con-  
24 sent.

1 (d) PERMITTED PURPOSES.—A covered entity, or  
2 service provider acting on behalf of a covered entity, may  
3 collect, process, retain, or transfer covered data for the  
4 following purposes, provided that the covered entity or  
5 service provider can demonstrate that the collection, proc-  
6 essing, retention, or transferring is necessary, propor-  
7 tionate, and limited to such purpose:

8 (1) To protect data security (as described in  
9 section 9), protect against spam, and maintain net-  
10 works and systems, including through diagnostics,  
11 debugging, and repairs.

12 (2) To comply with a legal obligation imposed  
13 by Federal, State, local, or Tribal law that is not  
14 preempted by this Act.

15 (3) To investigate, establish, prepare for, exer-  
16 cise, or defend cognizable legal claims on its own be-  
17 half.

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

22 (5) To effectuate a product recall pursuant to  
23 state or Federal law, or to fulfill a warranty.

24 (6) To conduct market research.

1           (7) With respect to covered data previously col-  
2 lected in accordance with this Act, to process such  
3 data into de-identified data, including to—

4           (A) develop or enhance a product or serv-  
5  ice of the covered entity;

6           (B) conduct internal research or analytics  
7 to improve a product or service of the covered  
8 entity; or

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

12           (i) is in the public interest; and

13           (ii) adheres to all relevant laws and  
14 regulations governing such research, in-  
15 cluding regulations for the protection of  
16 human subjects.

17           (8) To transfer assets to a third party in the  
18 context of a merger, acquisition, bankruptcy, or  
19 similar transaction when the third party assumes  
20 control, in whole or in part, of the covered entity's  
21 assets, only if the covered entity, in a reasonable  
22 time prior to such transfer, provides each affected  
23 individual with—

24           (A) a notice describing such transfer, in-  
25 cluding the name of any entity receiving the in-



1 individual's covered data and the privacy policies  
2 of such entity (as described in section 4); and

3 (B) a reasonable opportunity to—

4 (i) withdraw any previously given con-  
5 sent in accordance with the requirements  
6 of affirmative express consent under this  
7 Act related to the individual's covered  
8 data; and

9 (ii) request the deletion of the individ-  
10 ual's covered data, as described in section  
11 5.

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

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

1           (11) To prevent, detect, protect against, or re-  
2           spond to an ongoing or imminent network security  
3           or physical security incident, including an intrusion  
4           or trespass, medical alerts, fire alarms, or access  
5           control.

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

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

17          (14) Except with respect to sensitive covered  
18          data and only with respect to covered data pre-  
19          viously collected in accordance with this Act, to proc-  
20          ess such data as necessary to provide first party or  
21          contextual advertising by the covered entity for indi-  
22          viduals.

23          (15) Except with respect to sensitive covered  
24          data and only with respect to covered data pre-  
25          viously collected in accordance with this Act, for an

1 individual who has not opted out of targeted adver-  
2 tising pursuant to section 6, to process or transfer  
3 covered data to provide targeted advertising.

4 (e) GUIDANCE.—The Commission shall issue guid-  
5 ance regarding what is reasonably necessary and propor-  
6 tionate to comply with this section.

7 (f) JOURNALISM.—Nothing in this Act shall be con-  
8 strued to limit or diminish First Amendment freedoms  
9 guaranteed under the Constitution.

10 **SEC. 4. TRANSPARENCY.**

11 (a) IN GENERAL.—Each covered entity and service  
12 provider shall make publicly available, in a clear, con-  
13 spicuous, not misleading, easy-to-read, and readily acces-  
14 sible manner, a privacy policy that provides a detailed and  
15 accurate representation of the covered entity or service  
16 provider's data collection, processing, retention, and trans-  
17 fer activities.

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

21 (1) The identity and the contact information  
22 of—

23 (A) the covered entity or service provider  
24 to which the privacy policy applies (including  
25 the point of contact and a monitored email ad-

1 dress, as applicable, for data privacy and data  
2 security inquiries); and

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

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

9 or

10 (ii) has different contact information  
11 than the covered entity or service provider.

12 (2) With respect to the collection, processing,  
13 and retaining of covered data—

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

17 (B) the processing purposes for each such  
18 category of covered data.

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

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

1 (B) the name of each data broker to which  
2 the covered entity or service provider transfers  
3 covered data; and

4 (C) the purposes for which such data is  
5 transferred.

6 (4) The length of time the covered entity or  
7 service provider intends to retain each category of  
8 covered data, including sensitive covered data, or, if  
9 it is not possible to identify that time frame, the cri-  
10 teria used to determine the length of time the cov-  
11 ered entity or service provider intends to retain cat-  
12 egories of covered data.

13 (5) A prominent description of how an indi-  
14 vidual can exercise the rights described in sections 5  
15 and 6.

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

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

19 (8) Whether any covered data collected by the  
20 covered entity or service provider is transferred to,  
21 processed in, retained in, or otherwise accessible to  
22 a foreign adversary (as determined by the Secretary  
23 of Commerce in part 7.4 of title 15, Code of Federal  
24 Regulations, or any successor regulation).

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

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

6 (2) carries out activities related to such product  
7 or service.

8 (d) ACCESSIBILITY.—The covered entity or service  
9 provider shall provide the disclosures under this section  
10 in a manner that is reasonably accessible to and usable  
11 by individuals with disabilities.

12 (e) MATERIAL CHANGES.—

13 (1) NOTICE AND OPT OUT.—A covered entity  
14 that makes a material change to its privacy policy  
15 or practices with respect to previously collected cov-  
16 ered data shall—

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

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

21 (ii) a means to opt out of the proc-  
22 essing or transfer of such previously col-  
23 lected covered data pursuant to such mate-  
24 rial change; and

1 (B) with respect to the covered data of any  
2 individual who opts out using the means de-  
3 scribed in subparagraph (A)(ii), discontinue the  
4 processing or transfer of such previously col-  
5 lected covered data, except if such processing or  
6 transfer is strictly necessary to provide a prod-  
7 uct or service specifically requested by the indi-  
8 vidual.

9 (2) DIRECT NOTIFICATION.—The covered entity  
10 shall take all reasonable electronic measures to pro-  
11 vide direct notification, where possible, to each af-  
12 fected individual regarding material changes to the  
13 privacy policy, and such notification shall be pro-  
14 vided in each language in which the privacy policy  
15 is made available, taking into account available tech-  
16 nology and the nature of the relationship.

17 (3) CLARIFICATION.—Except as provided in  
18 paragraph (1)(B), nothing in this section shall be  
19 construed to affect the requirements for covered en-  
20 tities under section 3, 5, or 6.

21 (f) TRANSPARENCY REQUIREMENTS FOR LARGE  
22 DATA HOLDERS.—

23 (1) RETENTION OF PRIVACY POLICIES; LOG OF  
24 MATERIAL CHANGES.—Beginning after the date of  
25 enactment of this Act, each large data holder shall—

1 (A) retain and publish on the website of  
2 the large data holder a copy of each previous  
3 version of its privacy policy (as described in  
4 subsection (d)) for not less than 10 years; and

5 (B) make publicly available on its website,  
6 in a clear, conspicuous, and readily accessible  
7 manner, a log that describes the date and na-  
8 ture of each material change to its privacy pol-  
9 icy during such 10-year period in a manner  
10 that is sufficient for a reasonable individual to  
11 understand the effect of each material change.

12 (2) SHORT-FORM NOTICE TO CONSUMERS.—

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

18 (i) is concise, clear, and conspicuous  
19 and not misleading;

20 (ii) is readily accessible to the indi-  
21 vidual, based on the way an individual  
22 interacts with the large data holder and its  
23 products or services and what is reasonably  
24 anticipated within the context of the rela-



1                   tionship between the individual and the  
2                   large data holder;

3                   (iii) includes an overview of individual  
4                   rights and disclosures to reasonably draw  
5                   attention to data practices that may be un-  
6                   expected or that involve sensitive covered  
7                   data; and

8                   (iv) is not more than 500 words in  
9                   length.

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

17 **SEC. 5. INDIVIDUAL CONTROL OVER COVERED DATA.**

18                  (a) ACCESS TO, AND CORRECTION, DELETION, AND  
19                  PORTABILITY OF, COVERED DATA.—Subject to sub-  
20                  sections (b), (d), and (e), after receiving a verified request  
21                  from an individual, a covered entity shall provide the indi-  
22                  vidual with the right to—

23                         (1) access—

24                                 (A) in a format that be naturally read by  
25                                 a human, the covered data of the individual (or

1 an accurate representation of the covered data  
2 of the individual if the covered data is no longer  
3 in the possession of the covered entity or a serv-  
4 ice provider acting on behalf of the covered en-  
5 tity) that is collected, processed, or retained by  
6 the covered entity or any service provider of the  
7 covered entity;

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

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

17 (2) correct any inaccuracy or incomplete infor-  
18 mation with respect to the covered data of the indi-  
19 vidual that is collected, processed, or retained by the  
20 covered entity and, for covered data that has been  
21 transferred, notify any third party or service pro-  
22 vider to which the covered entity transferred such  
23 covered data of the corrected information;

24 (3) delete covered data of the individual that is  
25 collected, processed, or retained by the covered enti-

1 ty and, for covered data that has been transferred,  
2 request that the covered entity notify any third  
3 party or service provider to which the covered entity  
4 transferred such covered data of the individual's de-  
5 letion request; and

6 (4) to the extent technically feasible, export cov-  
7 ered data (except for derived data if the export of  
8 such derived data would result in the release of  
9 trade secrets or other proprietary or confidential  
10 data) of the individual that is collected, processed, or  
11 retained by the covered entity without licensing re-  
12 strictions that limit such transfers, in—

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

15 (B) a portable, structured, interoperable,  
16 and machine-readable format.

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

18 (1) shall provide an individual with the oppor-  
19 tunity to exercise each of the rights described in  
20 subsection (a); and

21 (2) with respect to—

22 (A) the first 3 times that an individual ex-  
23 ercises any right described in subsection (a)  
24 during any 12-month period, shall allow the in-

1           dividual to exercise such right free of charge;  
2           and

3                   (B) any time beyond the initial 3 times de-  
4           scribed in subparagraph (A), may charge a rea-  
5           sonable fee for each additional request to exer-  
6           cise any such right during such 12-month pe-  
7           riod.

8           (c) TIMING.—

9                   (1) IN GENERAL.—Subject to subsections (b),  
10          (d), and (e)—

11                   (A) any large data holder or data broker  
12          shall comply with a verified request from an in-  
13          dividual to exercise a right described in sub-  
14          section (a) not later than 15 calendar days  
15          after receiving such request, unless it is impos-  
16          sible or demonstrably impracticable to verify  
17          such individual; and

18                   (B) a covered entity that is not a large  
19          data holder shall comply with a verified request  
20          from an individual to exercise a right described  
21          in subsection (a) not later than 30 calendar  
22          days after receiving such request, unless it is  
23          impossible or demonstrably impracticable to  
24          verify such individual.

1           (2) EXTENSION.—The response period required  
2           under paragraph (1) may be extended once by not  
3           more than the applicable time period described in  
4           such paragraph when reasonably necessary, consid-  
5           ering the complexity and number of the individual’s  
6           requests, provided that the covered entity informs  
7           the individual of any such extension within the ini-  
8           tial response period, together with the reason for the  
9           extension.

10          (d) VERIFICATION.—

11           (1) IN GENERAL.—A covered entity shall verify  
12           that any individual requesting to exercise a right de-  
13           scribed in subsection (a) is—

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

16                   (B) an individual authorized to make such  
17                   a request on the individual’s behalf.

18           (2) ADDITIONAL INFORMATION.—If a covered  
19           entity cannot make the verification described in  
20           paragraph (1), the covered entity—

21                   (A) may request that the individual mak-  
22                   ing such request provide any additional infor-  
23                   mation necessary for the sole purpose of  
24                   verifying the identity of the individual; and

1           (B) shall not process, retain, or transfer  
2           such additional information for any other pur-  
3           pose.

4           (e) EXCEPTIONS.—

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

9           (A) cannot verify that the individual mak-  
10          ing such request is the individual whose covered  
11          data is the subject of the request or an indi-  
12          vidual authorized to make such a request on the  
13          individual's behalf;

14          (B) determines that exercise of the right  
15          would require access to another individual's  
16          sensitive covered data;

17          (C) determines that exercise of the right  
18          would require the correction or deletion of cov-  
19          ered data subject to a warrant, lawfully exe-  
20          cuted subpoena, or litigation hold notice in con-  
21          nection with such warrant or subpoena issued  
22          in a matter in which the covered entity is a  
23          named party;

24          (D) would violate Federal, State, local, or  
25          Tribal law that is not preempted by this Act;

1 (E) would violate the covered entity's pro-  
2 fessional ethical obligations;

3 (F) reasonably believes that the request is  
4 made in furtherance of fraud;

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

8 (H) reasonably believes that complying  
9 with the request would threaten data security.

10 (2) PERMISSIVE EXCEPTIONS.—

11 (A) IN GENERAL.—A covered entity may  
12 decline, with adequate explanation provided to  
13 the individual making the request, to comply  
14 with a request to exercise a right described in  
15 subsection (a), in whole or in part, if such com-  
16 pliance would—

17 (i) be demonstrably impossible due to  
18 technology or cost, and such adequate ex-  
19 planation includes a detailed description  
20 regarding the inability to comply with the  
21 request due to technology or cost;

22 (ii) delete covered data reasonably  
23 necessary to perform a contract between  
24 the covered entity and the individual;

1 (iii) with respect to a right described  
2 in paragraph (1) or (4) of subsection (a),  
3 require the covered entity to release trade  
4 secrets or other privileged, proprietary, or  
5 confidential business information;

6 (iv) prevent a covered entity from  
7 being able to maintain a confidential  
8 record of opt out requests pursuant to sec-  
9 tion 6, maintained solely for the purpose of  
10 preventing the covered data of an indi-  
11 vidual from being recollected after the indi-  
12 vidual submitted an opt out request; or

13 (v) with respect to deletion requests,  
14 require a private elementary or secondary  
15 school (as defined by State law) or a pri-  
16 vate institution of higher education (as de-  
17 fined by section 101 of the Higher Edu-  
18 cation Act of 1965 (20 U.S.C. 1001)) to  
19 delete covered data that would unreason-  
20 ably interfere with the provision of edu-  
21 cation services by or the ordinary operation  
22 of the school or institution.

23 (B) PARTIAL COMPLIANCE.—In the event  
24 a covered entity makes a permissive exception  
25 under subparagraph (A), the covered entity



1 shall partially comply with the remainder of the  
2 applicable request if partial compliance is pos-  
3 sible and not unduly burdensome.

4 (C) NUMBER OF REQUESTS.—For pur-  
5 poses of subparagraph (A)(i), the receipt of a  
6 large number of verified requests, on its own,  
7 shall not be considered to render compliance  
8 with a request demonstrably impossible.

9 (3) RULE OF CONSTRUCTION.—This section  
10 shall not require a covered entity to—

11 (A) retain covered data collected for a sin-  
12 gle, one-time transaction, if such covered data  
13 is not processed or transferred by the covered  
14 entity for any purpose other than completing  
15 such transaction;

16 (B) re-identify or attempt to re-identify de-  
17 identified data; or

18 (C) collect or retain any data in order to  
19 be capable of associating a verified individual's  
20 request with the covered data that is the sub-  
21 ject of the request.

22 (4) ADDITIONAL EXCEPTIONS.—

23 (A) IN GENERAL.—The Commission may  
24 promulgate regulations, in accordance with sec-  
25 tion 553 of title 5, United States Code, to es-

1           tablish additional permissive exceptions nec-  
2           essary to protect the rights of individuals, al-  
3           leviate undue burdens on covered entities, pre-  
4           vent unjust or unreasonable outcomes from the  
5           exercise of access, correction, deletion, or port-  
6           ability rights, or as otherwise necessary to fulfill  
7           the purposes of this section.

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

14          (C) CLARIFICATION.—A covered entity  
15          may not comply with an individual’s request to  
16          exercise a right under this section for any pur-  
17          pose the Commission identifies pursuant to this  
18          paragraph.

19          (5) ON-DEVICE DATA EXEMPTION.—A covered  
20          entity may decline to comply with a request to exer-  
21          cise a right described in paragraph (1), (2), or (3)  
22          of subsection (a), in whole or in part, if—

23                  (A) the covered data is exclusively on-de-  
24                  vice data; and

1 (B) the individual can exercise any such  
2 right using clear and conspicuous on-device con-  
3 trols.

4 (f) LARGE DATA HOLDER METRICS REPORTING.—

5 With respect to each calendar year for which an entity  
6 is considered a large data holder, such entity shall comply  
7 with the following reporting requirements:

8 (1) REQUIRED METRICS.—Compile the fol-  
9 lowing metrics for the prior calendar year:

10 (A) The number of verified access requests  
11 under subsection (a)(1).

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

14 (C) The number of requests to opt-out of  
15 covered data transfers under section 6(a)(1).

16 (D) The number of requests to opt-out of  
17 targeted advertising under section 6(a)(2).

18 (E) For each category of requests de-  
19 scribed in subparagraphs (A) through (D), the  
20 number of such requests that the large data  
21 holder complied with in whole or in part.

22 (F) For each category of requests de-  
23 scribed in subparagraphs (A) through (D), the  
24 average number of days within which such large

1 data holder substantively responded to the re-  
2 quest.

3 (2) PUBLIC DISCLOSURE.—Disclose by July 1  
4 of each applicable calendar year the information  
5 compiled under paragraph (1)—

6 (A) in such large data holder’s privacy pol-  
7 icy; or

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

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

16 (h) ACCESSIBILITY.—

17 (1) LANGUAGE.—A covered entity shall facili-  
18 tate the ability of individuals to make requests under  
19 subsection (a) in any language in which the covered  
20 entity provides a product or service.

21 (2) INDIVIDUALS WITH DISABILITIES.—The  
22 mechanisms by which a covered entity enables indi-  
23 viduals to make requests under subsection (a) shall  
24 be readily accessible and usable by individuals with  
25 disabilities.

1 **SEC. 6. OPT-OUT RIGHTS AND CENTRALIZED MECHANISM.**

2 (a) IN GENERAL.—Beginning on the effective date  
3 described in section 24, a covered entity shall provide to  
4 individuals the following opt-out rights:

5 (1) RIGHT TO OPT OUT OF COVERED DATA  
6 TRANSFERS.—A covered entity shall—

7 (A) provide an individual with a clear and  
8 conspicuous means to opt out of the transfer of  
9 the individual’s covered data;

10 (B) allow an individual to make an opt-out  
11 designation with respect to the transfer of the  
12 individual’s covered data through an opt-out  
13 mechanism as described in subsection (b); and

14 (C) abide by any such opt-out designation  
15 made by an individual and communicate such  
16 designation to all relevant service providers.

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

20 (A) provide an individual with a clear and  
21 conspicuous means to opt out of the processing  
22 of covered data in furtherance of targeted ad-  
23 vertising;

24 (B) allow an individual to make an opt-out  
25 designation with respect to targeted advertising

1 through an opt-out mechanism as described in  
2 subsection (b); and

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

6 (b) CENTRALIZED CONSENT AND OPT-OUT MECHA-  
7 NISM.—

8 (1) IN GENERAL.—Not later than 2 years after  
9 the date of enactment of this Act, the Commission  
10 shall, in consultation with the Secretary of Com-  
11 merce, promulgate regulations, in accordance with  
12 section 553 of title 5, United States Code, to estab-  
13 lish requirements and technical specifications for a  
14 privacy protective, centralized mechanism (including  
15 global privacy signals such as browser or device pri-  
16 vacy settings and registries of identifiers) for indi-  
17 viduals to exercise the opt-out rights established  
18 under this title, through a single interface that—

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

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

23 (ii) does not require that the indi-  
24 vidual provide additional information be-

1                   yond what is reasonably necessary to indi-  
2                   cate such preference;

3                   (iii) clearly represents an individual's  
4                   preference and is free of defaults con-  
5                   straining or presupposing such preference;

6                   (iv) is provided in any language in  
7                   which the covered entity provides products  
8                   or services subject to the opt out;

9                   (v) is provided in a manner that is  
10                  reasonably accessible to and usable by indi-  
11                  viduals with disabilities; and

12                  (vi) does not conflict with other com-  
13                  monly-used privacy settings or tools that  
14                  an individual may employ;

15                  (B) provides a mechanism for the indi-  
16                  vidual to selectively opt out of the covered enti-  
17                  ty's collection, processing, retention, or transfer  
18                  of covered data, without affecting the individ-  
19                  ual's preferences with respect to other entities  
20                  or disabling the opt-out preference signal glob-  
21                  ally;

22                  (C) states that, in the case of a page or  
23                  setting view that the individual accesses to set  
24                  the opt-out preference signal, the individual

1 should see up to 2 choices, corresponding to the  
2 rights established under subsection (a); and

3 (D) ensures that the opt-out preference  
4 signal applies neutrally.

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

10 **SEC. 7. INTERFERENCE WITH CONSUMER RIGHTS.**

11 (a) DARK PATTERNS PROHIBITED.—

12 (1) IN GENERAL.—A covered entity shall not  
13 use dark patterns to—

14 (A) divert an individual’s attention from  
15 any notice required under this Act;

16 (B) impair an individual’s ability to exer-  
17 cise any right under this Act; or

18 (C) obtain, infer, or facilitate an individ-  
19 ual’s consent for any action that requires an in-  
20 dividual’s consent under this Act.

21 (2) CLARIFICATION.—Any agreement by an in-  
22 dividual that is obtained, inferred, or facilitated  
23 through dark patterns shall not constitute consent  
24 for any purpose.



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

7 **SEC. 8. PROHIBITION ON DENIAL OF SERVICE AND WAIVER**  
8 **OF RIGHTS.**

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

16 (b) RULES OF CONSTRUCTION.—

17 (1) BONA FIDE LOYALTY PROGRAMS.—

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

21 (i) a different price, rate, level, qual-  
22 ity, or selection of products or services to  
23 an individual, including offering products  
24 or services for no fee, if the offering is in  
25 connection with an individual's voluntary

1 participation in a bona fide loyalty pro-  
2 gram, provided that—

3 (I) the individual provided af-  
4 firmative express consent to partici-  
5 pate in such bona fide loyalty pro-  
6 gram;

7 (II) the covered entity provides  
8 an individual with means to withdraw  
9 the affirmative express consent pre-  
10 viously provided by the individual in  
11 the manner set forth in section  
12 3(b)(2);

13 (III) the covered entity abides by  
14 an individual's exercise of any right  
15 described in sections 3(b)(2), 5, or 6;  
16 and

17 (IV) the individual provides af-  
18 firmative express consent for the  
19 transfer of any data collected in con-  
20 nection with a bona fide loyalty pro-  
21 gram; and

22 (ii) different prices or functionalities  
23 with respect to a product or service based  
24 on an individual's decision to terminate  
25 membership in a bona fide loyalty program

1 or to exercise a right under section 5(a)(3)  
2 that deletes covered data that is strictly  
3 necessary for participation in the bona fide  
4 loyalty program.

5 (B) BONA FIDE LOYALTY PROGRAM DE-  
6 FINED.—For purposes of this paragraph, the  
7 term “bona fide loyalty program” includes re-  
8 wards, premium features, discounts, or club  
9 card programs offered by a covered entity that  
10 is not a covered high-impact social media com-  
11 pany or data broker.

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

17 (3) DECLINING A PRODUCT OR SERVICE.—  
18 Nothing in subsection (a) may be construed to pro-  
19 hibit a covered entity from declining to provide a  
20 product or service insofar as the collection and proc-  
21 essing of covered data is strictly necessary for the  
22 function of such product or service.

1 **SEC. 9. DATA SECURITY AND PROTECTION OF COVERED**  
2 **DATA.**

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

5 (1) IN GENERAL.—A covered entity and service  
6 provider shall establish, implement, and maintain  
7 reasonable data security practices to protect—

8 (A) the confidentiality, integrity, and ac-  
9 cessibility of covered data; and

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

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

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

17 (B) the nature and scope of the covered  
18 entity's or the service provider's collecting,  
19 processing, retaining, or transferring of covered  
20 data, taking into account such covered entity's  
21 or service provider's changing business oper-  
22 ations with respect to covered data;

23 (C) the volume, nature, and sensitivity of  
24 the covered data at issue; and

25 (D) the state-of-the-art (and limitations  
26 thereof) in administrative, technical, and phys-

1           ical safeguards for protecting such covered  
2           data.

3           (b) SPECIFIC REQUIREMENTS.—The data security  
4 practices required under subsection (a) shall include, for  
5 each respective entity’s own system, at a minimum, the  
6 following practices:

7           (1) ASSESS VULNERABILITIES.—Routinely iden-  
8           tifying and assessing any reasonably foreseeable in-  
9           ternal or external risk to, and vulnerability in, each  
10          system maintained by the covered entity or service  
11          provider that collects, processes, retains, or transfers  
12          covered data, including unauthorized access to or  
13          corruption of such covered data, human  
14          vulnerabilities, access rights, and the use of service  
15          providers. Such activities shall include a plan to re-  
16          ceive and consider unsolicited reports of vulnerability  
17          by any entity or individual, and, if such report is  
18          reasonably credible, perform a reasonable and timely  
19          investigation of such report and take appropriate ac-  
20          tion necessary to protect covered data against such  
21          vulnerability.

22          (2) PREVENTATIVE AND CORRECTIVE AC-  
23          TION.—

24                  (A) IN GENERAL.—Taking preventative  
25                  and corrective action to mitigate any reasonably

1           foreseeable internal or external risk or vulner-  
2           ability to covered data identified by the covered  
3           entity or service provider, consistent with the  
4           nature of such risk or vulnerability and the cov-  
5           ered entity's or service provider's role in col-  
6           lecting, processing, retaining, or transferring  
7           the data, which may include implementing ad-  
8           ministrative, technical, or physical safeguards  
9           or changes to data security practices or the ar-  
10          chitecture, installation, or implementation of  
11          network or operating software.

12                   (B) EVALUATION OF PREVENTATIVE AND  
13                   CORRECTIVE ACTION.—Evaluating and making  
14                   reasonable adjustments to the action described  
15                   in subparagraph (A) in light of any material  
16                   changes in technology, internal or external  
17                   threats to covered data, and the covered entity's  
18                   or service provider's changing business oper-  
19                   ations with respect to covered data.

20                   (3) INFORMATION RETENTION AND DIS-  
21                   POSAL.—Disposing of covered data (either by or at  
22                   the direction of a covered entity) that is required to  
23                   be deleted by law or is no longer necessary for the  
24                   purpose for which the data was collected, processed,  
25                   retained, or transferred, unless an individual has

1 provided affirmative express consent to such reten-  
2 tion. Such disposal shall include destroying, perma-  
3 nently erasing, or otherwise modifying the covered  
4 data to make such data permanently unreadable or  
5 indecipherable and unrecoverable to ensure ongoing  
6 compliance with this section.

7 (4) RETENTION SCHEDULE.—Developing, main-  
8 taining, and adhering to a retention schedule for  
9 covered data disposal consistent with the practices  
10 and procedures required in paragraph (3).

11 (5) TRAINING.—Training each employee with  
12 access to covered data on how to safeguard covered  
13 data and updating such training as necessary.

14 (6) INCIDENT RESPONSE.—Implementing pro-  
15 cedures to detect, respond to, and recover from data  
16 security incidents, including breaches of data secu-  
17 rity.

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

23 **SEC. 10. EXECUTIVE RESPONSIBILITY.**

24 (a) DESIGNATION OF PRIVACY AND DATA SECURITY  
25 OFFICERS.—

1 (1) DESIGNATION.—

2 (A) IN GENERAL.—Except for an entity  
3 that is a large data holder, a covered entity or  
4 service provider shall designate 1 or more quali-  
5 fied employees to serve as privacy or data secu-  
6 rity officers.

7 (B) REQUIREMENTS FOR OFFICERS.—An  
8 employee who is designated by a covered entity  
9 or service provider as a privacy or data security  
10 officer shall, at a minimum—

11 (i) implement a data privacy program  
12 and data security program to safeguard  
13 the privacy and security of covered data in  
14 compliance with the requirements of this  
15 Act; and

16 (ii) facilitate the covered entity's or  
17 service provider's ongoing compliance with  
18 this Act.

19 (2) REQUIREMENTS FOR LARGE DATA HOLD-  
20 ERS.—

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



1 (B) ANNUAL CERTIFICATION.—

2 (i) IN GENERAL.—Beginning 1 year  
3 after the date of enactment of this Act, the  
4 chief executive officer of a large data hold-  
5 er (or, if the large data holder does not  
6 have a chief executive officer, the highest  
7 ranking officer of the large data holder)  
8 and each privacy officer and data security  
9 officer of such large data holder designated  
10 under subparagraph (A) shall annually cer-  
11 tify to the Commission, in a manner speci-  
12 fied by the Commission, that the large  
13 data holder maintains—

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

16 (II) internal reporting structures  
17 (as described in subparagraph (C)) to  
18 ensure that such certifying officers  
19 are involved in, and responsible for,  
20 decisions that impact compliance by  
21 the large data holder with this Act.

22 (ii) REQUIREMENTS.—A certification  
23 submitted under clause (i) shall be based  
24 on a review of the effectiveness of a large  
25 data holder’s internal controls and report-

1                   ing structures that is conducted by the cer-  
2                   tifying officers not more than 90 days be-  
3                   fore the submission of the certification.

4                   (C) INTERNAL REPORTING STRUCTURE RE-  
5                   QUIREMENTS.—At least 1 of the officers de-  
6                   scribed in subparagraph (A) shall, either di-  
7                   rectly or through a supervised designee—

8                   (i) establish processes to periodically  
9                   review and update the privacy and security  
10                  policies, practices, and procedures of the  
11                  large data holder, as necessary;

12                  (ii) conduct biennial and comprehen-  
13                  sive audits to ensure the policies, practices,  
14                  and procedures of the large data holder  
15                  comply with this Act and, upon request,  
16                  make such audits available to the Commis-  
17                  sion;

18                  (iii) develop a program to educate and  
19                  train employees about the requirements of  
20                  this Act;

21                  (iv) maintain updated, accurate, clear,  
22                  and understandable records of all material  
23                  privacy and data security practices of the  
24                  large data holder; and

1 (v) serve as the point of contact be-  
2 tween the large data holder and enforce-  
3 ment authorities.

4 (D) PRIVACY IMPACT ASSESSMENTS.—

5 (i) IN GENERAL.—Not later than 1  
6 year after the date of enactment of this  
7 Act or 1 year after the date that an entity  
8 first meets the definition of large data  
9 holder, whichever is earlier, and biennially  
10 thereafter, each large data holder shall  
11 conduct a privacy impact assessment that  
12 weighs the benefits of the entity's covered  
13 data collection, processing, retention, and  
14 transfer practices against the potential ad-  
15 verse consequences of such practices to in-  
16 dividual privacy.

17 (ii) ASSESSMENT REQUIREMENTS.—A  
18 privacy impact assessment required under  
19 clause (i) shall be—

20 (I) reasonable and appropriate in  
21 scope given—

22 (aa) the nature and volume  
23 of the covered data collected,  
24 processed, retained, or trans-

1                   ferred by the large data holder;  
2                   and

3                   (bb) the potential risks  
4                   posed to the privacy of individ-  
5                   uals by the collection, processing,  
6                   retention, and transfer of covered  
7                   data by the large data holder;

8                   (II) documented in written form  
9                   and maintained by the large data  
10                  holder, unless rendered out of date by  
11                  a subsequent assessment conducted  
12                  under clause (i); and

13                  (III) approved by the privacy of-  
14                  ficer of the large data holder.

15                  (iii) ADDITIONAL FACTORS TO IN-  
16                  CLUDE IN ASSESSMENT.—In assessing the  
17                  privacy risks, the large data holder shall  
18                  include reviews of the means by which  
19                  emerging technologies, including  
20                  blockchain, distributed ledger technologies,  
21                  privacy enhancing technologies, and other  
22                  emerging technologies are used to secure  
23                  covered data.

24 **SEC. 11. SERVICE PROVIDERS AND THIRD PARTIES.**

25                  (a) SERVICE PROVIDERS.—

1 (1) IN GENERAL.—A service provider—

2 (A) shall adhere to the instructions of a  
3 covered entity and only collect, process, retain,  
4 or transfer service provider data to the extent  
5 necessary, proportionate, and limited to provide  
6 a service requested by the covered entity, as set  
7 out in the contract required under paragraph  
8 (2);

9 (B) may not collect, process, retain, or  
10 transfer covered data if the service provider has  
11 actual knowledge that a covered entity violated  
12 this Act with respect to such data;

13 (C) shall assist a covered entity in fulfilling  
14 the covered entity's obligations to respond to  
15 consumer rights requests pursuant to sections  
16 5, 6, and 14 by appropriate technical and orga-  
17 nizational measures, taking into account the na-  
18 ture of the processing and the information rea-  
19 sonably available to the service provider;

20 (D) shall, upon the reasonable request of  
21 the covered entity, make available to the cov-  
22 ered entity information necessary to dem-  
23 onstrate the service provider's compliance with  
24 the requirements of this Act;

1           (E) shall delete or return, as directed by  
2           the covered entity, all covered data as soon as  
3           practicable after the contractually agreed upon  
4           end of the provision of services, unless the serv-  
5           ice provider's retention of the covered data is  
6           required by law;

7           (F) may engage another service provider  
8           for purposes of processing or retaining covered  
9           data on behalf of a covered entity only after ex-  
10          ercising reasonable due diligence in selecting  
11          such other service provider as required by sub-  
12          section (d), providing such covered entity with  
13          written notice of the engagement, and pursuant  
14          to a written contract that requires such other  
15          service provider to satisfy the requirements of  
16          this Act with respect to covered data;

17          (G) shall develop, implement, and maintain  
18          reasonable administrative, technical, and phys-  
19          ical safeguards that are designed to protect the  
20          security and confidentiality of covered data the  
21          service provider processes consistent with sec-  
22          tion 9; and

23          (H) shall—

24                  (i) allow and cooperate with reason-  
25                  able assessments by the covered entity; or

1                   (ii) arrange for a qualified and inde-  
2                   pendent assessor to conduct an assessment  
3                   of the service provider's policies and tech-  
4                   nical and organizational measures in sup-  
5                   port of the obligations under this Act,  
6                   using an appropriate and accepted control  
7                   standard or framework and assessment  
8                   procedure for such assessments and report  
9                   the results of such assessment to the cov-  
10                  ered entity.

11                  (2) CONTRACT REQUIREMENTS.—A contract be-  
12                  tween a covered entity and a service provider—

13                         (A) shall govern the service provider's data  
14                         processing procedures with respect to any col-  
15                         lection, processing, retention, or transfer per-  
16                         formed on behalf of the covered entity;

17                         (B) shall clearly set forth—

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

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

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

24                                 (iv) the duration of the processing or  
25                                 retention; and

1 (v) the rights and obligations of both  
2 parties;

3 (C) shall not relieve a covered entity or  
4 service provider of any obligation under this  
5 Act; and

6 (D) shall prohibit—

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

11 (ii) combining service provider data  
12 with covered data which the service pro-  
13 vider receives from or on behalf of another  
14 entity or collects from the interaction of  
15 the service provider with an individual,  
16 provided that such combining is not nec-  
17 essary to effectuate a purpose described in  
18 section 3(d) and is otherwise permitted  
19 under the contract required by this sub-  
20 section.

21 (b) THIRD PARTIES.—A third party—

22 (1) shall not process, retain, or transfer third-  
23 party data for a purpose other than—

24 (A) in the case of sensitive covered data,  
25 the purpose for which an individual gave af-



1 firmative express consent for the transfer of the  
2 individual's sensitive covered data; or

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

7 (2) for purposes of paragraph (1), may reason-  
8 ably rely on representations made by the covered en-  
9 tity that transferred the third-party data regarding  
10 the expectations of a reasonable person based on dis-  
11 closures by the covered entity about the treatment of  
12 such data, provided that the third party conducts  
13 reasonable due diligence on the representations of  
14 the covered entity and finds those representations to  
15 be credible; and

16 (3) shall be exempt from the requirements of  
17 section 3(b) with respect to third-party data, but  
18 shall otherwise have the same responsibilities and  
19 obligations as a covered entity with respect to such  
20 data under all other provisions of this Act.

21 (c) RULES OF CONSTRUCTION.—

22 (1) SUCCESSIVE ACTOR VIOLATIONS.—

23 (A) IN GENERAL.—With respect to a viola-  
24 tion of this Act by a service provider or third  
25 party regarding covered data received by the

1 service provider or third party from a covered  
2 entity, the covered entity that transferred such  
3 covered data to the service provider or third  
4 party shall not be in violation of this Act if the  
5 covered entity transferred the covered data to  
6 the service provider or third party in compli-  
7 ance with the requirements of this Act and, at  
8 the time of transferring such covered data, the  
9 entity did not have actual knowledge, or reason  
10 to believe, that the service provider or third  
11 party intended to violate this Act.

12 (B) KNOWLEDGE OF VIOLATION.—An enti-  
13 ty that transfers covered data to a service pro-  
14 vider or third party and has actual knowledge,  
15 or reason to believe, that such service provider  
16 or third party is violating, or is about to violate,  
17 the requirements of this Act shall immediately  
18 cease the transfer of covered data to such serv-  
19 ice provider or third party.

20 (2) PRIOR ACTOR VIOLATIONS.—An entity that  
21 collects, processes, retains, or transfers covered data  
22 in compliance with the requirements of this Act shall  
23 not be in violation of this Act as a result of a viola-  
24 tion by an entity from which it receives, or on whose

1       behalf it collects, processes, retains, or transfers,  
2       covered data.

3       (d) DUE DILIGENCE.—

4             (1) SERVICE PROVIDER SELECTION.—A covered  
5       entity shall exercise reasonable due diligence in se-  
6       lecting a service provider.

7             (2) TRANSFER TO THIRD PARTY.—A covered  
8       entity shall exercise reasonable due diligence in de-  
9       ciding to transfer covered data to a third party.

10            (3) GUIDANCE.—Not later than 2 years after  
11       the date of enactment of this Act, the Commission  
12       shall publish guidance regarding compliance with  
13       this subsection.

14   **SEC. 12. DATA BROKERS.**

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

16             (1) establish and maintain a publicly accessible  
17       website; and

18             (2) place a clear, conspicuous, not misleading,  
19       and readily accessible notice on the publicly acces-  
20       sible website and any mobile application of the data  
21       broker that—

22                (A) the entity is a data broker, using spe-  
23       cific language that the Commission shall de-  
24       velop through guidance not later than 180 days  
25       after the date of enactment of this Act;

1 (B) an individual has a right to exercise  
2 the rights described in sections 5 and 6, includ-  
3 ing a link or other tool to allow an individual  
4 to exercise such rights;

5 (C) includes a link to the website estab-  
6 lished under subsection (c)(3); and

7 (D) is reasonably accessible to and usable  
8 by individuals with disabilities.

9 (b) PROHIBITED PRACTICES.—A data broker is pro-  
10 hibited from—

11 (1) advertising or marketing the access to or  
12 transfer of covered data for the purposes of—

13 (A) stalking or harassing another indi-  
14 vidual; or

15 (B) engaging in fraud, identity theft, or  
16 unfair or deceptive acts or practices; or

17 (2) misrepresenting the business practices of  
18 the data broker.

19 (c) DATA BROKER REGISTRATION.—

20 (1) IN GENERAL.—Not later than January 31  
21 of each calendar year that follows a calendar year  
22 during which an entity acted as a data broker with  
23 respect to more than 5,000 individuals or devices  
24 that identify or are linked or reasonably linkable to

1 an individual, such 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  
5 paragraph (1), a data broker shall do the following:

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

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

10 (i) The legal name and primary phys-  
11 ical, email, and internet addresses of the  
12 data broker.

13 (ii) A description of the categories of  
14 covered data the data broker collects, proc-  
15 esses, retains, and transfers.

16 (iii) The contact information of the  
17 data broker, including the name of a con-  
18 tact person, a monitored telephone num-  
19 ber, a monitored e-mail address, a website,  
20 and a physical mailing address.

21 (iv) A link to a website through which  
22 an individual may easily exercise the rights  
23 described in subsection (a)(2)(B).

24 (3) DATA BROKER REGISTRY.—

1           (A) ESTABLISHMENT.—The Commission  
2 shall establish and maintain on a publicly avail-  
3 able website a searchable registry of data bro-  
4 kers that are registered with the Commission  
5 under this subsection.

6           (B) REQUIREMENTS.—The registry estab-  
7 lished under subparagraph (A) shall—

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

10                (ii) include the information required  
11 under paragraph (2)(B) for each data  
12 broker; and

13                (iii) includes a mechanism by which  
14 an individual may submit a request to all  
15 registered data brokers that are not con-  
16 sumer reporting agencies (as defined in  
17 section 603(f) of the Fair Credit Reporting  
18 Act (15 U.S.C. 1681a(f))), and to the ex-  
19 tent such third-party collecting entities are  
20 not acting as consumer reporting agencies  
21 (as so defined), a “Do Not Collect” direc-  
22 tive such that any registered data broker  
23 shall ensure that the data broker no longer  
24 collects covered data related to such indi-  
25 vidual without the affirmative express con-

1 sent of such individual, except insofar as  
2 the data broker is acting as a service pro-  
3 vider.

4 (4) DO NOT COLLECT REQUESTS.—

5 (A) COMPLIANCE.—Subject to subpara-  
6 graph (B), each data broker that receives a re-  
7 quest from an individual using the mechanism  
8 established under paragraph (3)(B)(iii) shall  
9 comply with such request not later than 30  
10 days after receiving such request.

11 (B) EXCEPTION.—A data broker may de-  
12 cline to fulfill a request from an individual  
13 where—

14 (i) the data broker has actual knowl-  
15 edge that the individual has been convicted  
16 of a crime related to the abduction or sex-  
17 ual exploitation of a child; and

18 (ii) the data collected by the data  
19 broker is necessary—

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

22 (II) for the Congressionally des-  
23 igned entity that serves as the non-  
24 profit national resource center and  
25 clearinghouse to provide assistance to

1 victims, families, child-serving profes-  
2 sionals, and the general public regard-  
3 ing issues related to missing and ex-  
4 ploited children.

5 (d) PENALTIES.—

6 (1) IN GENERAL.—Subject to paragraph (2), a  
7 data broker that violates this section shall be liable  
8 for civil penalties as set forth in subsections (l) and  
9 (m) of section 5 of the Federal Trade Commission  
10 Act, (15 U.S.C. 45(l), (m)).

11 (2) EXCEPTIONS.—A data broker that—

12 (A) fails to register with the Commission  
13 as required by subsection (c) shall be liable  
14 for—

15 (i) a civil penalty of \$100 for each day  
16 the data broker fails to register, not to ex-  
17 ceed a total of \$10,000 for any year; and

18 (ii) an amount equal to the registra-  
19 tion fee due under subsection (c)(2)(A) for  
20 each year that the data broker failed to  
21 register as required under subsection  
22 (c)(1); or

23 (B) fails to provide notice as required by  
24 subsection (a) shall be liable for a civil penalty  
25 of \$100 for each day the data broker fails to



1           provide such notice, not to exceed a total of  
2           \$10,000 for any year.

3           (3) RULE OF CONSTRUCTION.—Except as set  
4           forth in paragraph (2), nothing in this subsection  
5           shall be construed as altering, limiting, or affecting  
6           any enforcement authority or remedy provided under  
7           this Act.

8 **SEC. 13. CIVIL RIGHTS AND ALGORITHMS.**

9           (a) CIVIL RIGHTS PROTECTIONS.—

10           (1) IN GENERAL.—A covered entity or a service  
11           provider may not collect, process, retain, or transfer  
12           covered data in a manner that discriminates in or  
13           otherwise makes unavailable the equal enjoyment of  
14           goods or services on the basis of race, color, religion,  
15           national origin, sex, or disability.

16           (2) EXCEPTIONS.—This subsection shall not  
17           apply to—

18           (A) the collection, processing, retention, or  
19           transfer of covered data for the purpose of—

20           (i) a covered entity's or a service pro-  
21           vider's self-testing to prevent or mitigate  
22           unlawful discrimination; or

23           (ii) diversifying an applicant, partici-  
24           pant, or customer pool;

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

5 (C) advertising, marketing, or soliciting  
6 economic opportunities or benefits to underrep-  
7 resented populations or members of protected  
8 classes as described in paragraph (1).

9 (b) FTC ENFORCEMENT ASSISTANCE.—

10 (1) IN GENERAL.—Whenever the Commission  
11 obtains information that a covered entity or service  
12 provider may have collected, processed, retained, or  
13 transferred covered data in violation of subsection  
14 (a), the Commission shall transmit such information  
15 as allowable under Federal law to any Executive  
16 agency with authority to initiate enforcement actions  
17 or proceedings relating to such violation.

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

22 (A) the types of information the Commis-  
23 sion transmitted to Executive agencies under  
24 paragraph (1) during the previous 1-year pe-  
25 riod; and

1                   (B) how such information relates to Fed-  
2                   eral civil rights laws.

3                   (3) TECHNICAL ASSISTANCE.—In transmitting  
4                   information under paragraph (1), the Commission  
5                   may consult and coordinate with, and provide tech-  
6                   nical and investigative assistance, as appropriate, to  
7                   such Executive agency.

8                   (4) COOPERATION WITH OTHER AGENCIES.—  
9                   The Commission may implement this subsection by  
10                  executing agreements or memoranda of under-  
11                  standing with the appropriate Executive agencies.

12                  (c) COVERED ALGORITHM IMPACT AND EVALUA-  
13                  TION.—

14                  (1) COVERED ALGORITHM IMPACT ASSESS-  
15                  MENT.—

16                  (A) IMPACT ASSESSMENT.—Notwith-  
17                  standing any other provision of law, not later  
18                  than 2 years after the date of enactment of this  
19                  Act, and annually thereafter, a large data hold-  
20                  er that uses a covered algorithm in a manner  
21                  that poses a consequential risk of a harm iden-  
22                  tified under subparagraph (B)(vi) to an indi-  
23                  vidual or group of individuals and uses such  
24                  covered algorithm, solely or in part, to collect,  
25                  process, or transfer covered data shall conduct

1 an impact assessment of such algorithm in ac-  
2 cordance with subparagraph (B).

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

6 (i) A detailed description of the design  
7 process and methodologies of the covered  
8 algorithm.

9 (ii) A statement of the purpose and  
10 proposed uses of the covered algorithm.

11 (iii) A detailed description of the data  
12 used by the covered algorithm, including  
13 the specific categories of data that will be  
14 processed as input and any data used to  
15 train the model that the covered algorithm  
16 relies on, if applicable.

17 (iv) A description of the outputs pro-  
18 duced by the covered algorithm.

19 (v) An assessment of the necessity  
20 and proportionality of the covered algo-  
21 rithm in relation to its stated purpose.

22 (vi) A detailed description of steps the  
23 large data holder has taken or will take to  
24 mitigate potential harms from the covered

1 algorithm to an individual or group of indi-  
2 viduals, including related to—

3 (I) covered minors;

4 (II) making or facilitating adver-  
5 tising for, or determining access to, or  
6 restrictions on the use of housing,  
7 education, employment, healthcare, in-  
8 surance, or credit opportunities;

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

16 (IV) disparate impact on the  
17 basis of individuals' race, color, reli-  
18 gion, national origin, sex, or disability  
19 status; or

20 (V) disparate impact on the basis  
21 of individuals' political party registra-  
22 tion status.

23 (2) ALGORITHM DESIGN EVALUATION.—Not-  
24 withstanding any other provision of law, not later  
25 than 2 years after the date of enactment of this Act,

1 a covered entity or service provider that knowingly  
2 develops a covered algorithm shall, prior to deploy-  
3 ing the covered algorithm in interstate commerce,  
4 evaluate the design, structure, and inputs of the cov-  
5 ered algorithm, including any training data used to  
6 develop the covered algorithm, to reduce the risk of  
7 the potential harms identified under paragraph  
8 (1)(B)(vi).

9 (3) OTHER CONSIDERATIONS.—

10 (A) FOCUS.—In complying with para-  
11 graphs (1) and (2), a covered entity and a serv-  
12 ice provider may focus the impact assessment  
13 or evaluation on any covered algorithm, or por-  
14 tions of a covered algorithm, that will be put to  
15 use and may reasonably contribute to the risk  
16 of the potential harms identified under para-  
17 graph (1)(B)(vi).

18 (B) AVAILABILITY.—

19 (i) IN GENERAL.—A covered entity  
20 and a service provider—

21 (I) shall, not later than 30 days  
22 after completing an impact assess-  
23 ment or evaluation under paragraph  
24 (1) or (2), submit the impact assess-

1                   ment or evaluation to the Commis-  
2                   sion;

3                   (II) shall, upon request, make  
4                   such impact assessment and evalua-  
5                   tion available to Congress; and

6                   (III) may make a summary of  
7                   such impact assessment and evalua-  
8                   tion publicly available in a place that  
9                   is easily accessible to individuals.

10                  (ii) TRADE SECRETS.—A covered enti-  
11                  ty or service provider may redact and seg-  
12                  regate any trade secret (as defined in sec-  
13                  tion 1839 of title 18, United States Code)  
14                  or other confidential or proprietary infor-  
15                  mation from public disclosure under this  
16                  subparagraph, and the Commission shall  
17                  abide by its obligations under section 6(f)  
18                  of the Federal Trade Commission Act (15  
19                  U.S.C. 46(f)) with respect to such informa-  
20                  tion.

21                  (C) LIMITATION ON ENFORCEMENT.—

22                  (i) IN GENERAL.—Subject to clause  
23                  (ii), the Commission may not use any in-  
24                  formation obtained solely and exclusively  
25                  through a covered entity or a service pro-

1 vider’s disclosure of information to the  
2 Commission in compliance with this section  
3 for any purpose other than to carry out  
4 the provisions of this Act, including the  
5 study and report described in paragraph  
6 (6).

7 (ii) EXCEPTIONS.—

8 (I) PROVISION TO CONGRESS.—

9 The limitation described in clause (i)  
10 does not preclude the Commission  
11 from providing such information to  
12 Congress in response to a subpoena.

13 (II) CONSENT ORDERS.—The

14 limitation described in clause (i) does  
15 not preclude the Commission from en-  
16 forcing a consent order entered into  
17 with the applicable covered entity or  
18 service provider.

19 (4) GUIDANCE.—Not later than 2 years after  
20 the date of enactment of this Act, the Commission  
21 shall, in consultation with the Secretary of Com-  
22 merce, publish guidance regarding compliance with  
23 this section.

24 (5) RULEMAKING AND EXEMPTION.—The Com-  
25 mission may promulgate regulations, in accordance



1 with section 553 of title 5, United States Code, as  
2 necessary to establish processes by which a—

3 (A) large data holder shall submit an im-  
4 pact assessment to the Commission under para-  
5 graph (3)(B)(i)(I); and

6 (B) large data holder, covered entity, or  
7 service provider may exclude from this sub-  
8 section any covered algorithm that presents low  
9 or minimal risk of the potential harms identi-  
10 fied under paragraph (1)(B)(vi) to an individual  
11 or group of individuals.

12 (6) STUDY AND REPORT.—

13 (A) STUDY.—The Commission, in con-  
14 sultation with the Secretary of Commerce, shall  
15 conduct a study, to review any impact assess-  
16 ment or evaluation submitted under this sub-  
17 section. Such study shall include an examina-  
18 tion of—

19 (i) best practices for the assessment  
20 and evaluation of covered algorithms; and

21 (ii) methods to reduce the risk of  
22 harm to individuals that may be related to  
23 the use of covered algorithms.

24 (B) REPORT.—

1 (i) INITIAL REPORT.—Not later than  
2 3 years after the date of enactment of this  
3 Act, the Commission, in consultation with  
4 the Secretary of Commerce, shall submit to  
5 Congress a report containing the results of  
6 the study conducted under subparagraph  
7 (A), together with recommendations for  
8 such legislation and administrative action  
9 as the Commission determines appropriate.

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

16 **SEC. 14. CONSEQUENTIAL DECISION OPT OUT.**

17 (a) IN GENERAL.—An entity that uses a covered al-  
18 gorithm to make or facilitate a consequential decision  
19 shall—

20 (1) provide—

21 (A) notice to any individual subject to such  
22 use of the covered algorithm; and

23 (B) an opportunity for the individual to  
24 opt out of such use of the covered algorithm;  
25 and

1           (2) abide by any opt-out designation made by  
2           an individual under paragraph (1)(B).

3           (b) NOTICE.—The notice required under subsection  
4 (a)(1)(A) shall—

5           (1) be clear, conspicuous, and not misleading;

6           (2) provide meaningful information about how  
7           the covered algorithm makes or facilitates a con-  
8           sequential decision, including the range of potential  
9           outcomes;

10          (3) be provided in each language in which the  
11          entity—

12                 (A) provides a product or service subject to  
13                 the use of such covered algorithm; or

14                 (B) carries out activities related to such  
15                 product or service; and

16          (4) be reasonably accessible to and usable by in-  
17          dividuals with disabilities.

18          (c) GUIDANCE.—Not later than 2 years after the date  
19 of enactment of this Act, the Commission, in consultation  
20 with the Secretary of Commerce, shall publish guidance  
21 regarding compliance with this section.

22          (d) CONSEQUENTIAL DECISION DEFINED.—For the  
23 purposes of this section, the term “consequential decision”  
24 means a determination or an offer, including through ad-  
25 vertisement, that uses covered data and relates to—

1 (1) an individual's or a class of individuals' ac-  
2 cess to or equal enjoyment of housing, employment,  
3 education enrollment or opportunity, healthcare, in-  
4 surance, or credit opportunities; or

5 (2) access to, or restrictions on the use of, any  
6 place of public accommodation.

7 **SEC. 15. COMMISSION APPROVED COMPLIANCE GUIDE-**  
8 **LINES.**

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

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

17 (2) APPLICATION REQUIREMENTS.—Such appli-  
18 cation shall include—

19 (A) a description of how the proposed com-  
20 pliance guidelines will meet or exceed the re-  
21 quirements of this Act;

22 (B) a description of the entities or activi-  
23 ties the proposed set of compliance guidelines is  
24 designed to cover;

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

4 (D) a description of the independent orga-  
5 nization, which shall not be associated with any  
6 of the participating covered entities, that will  
7 administer the compliance guidelines; and

8 (E) and a description of how such entities  
9 will be assessed for adherence to such compli-  
10 ance guidelines by the independent organization  
11 described in subparagraph (D).

12 (3) COMMISSION REVIEW.—

13 (A) INITIAL APPROVAL.—

14 (i) PUBLIC COMMENT PERIOD.—Not  
15 later than 90 days after receiving an appli-  
16 cation under paragraph (1), the Commis-  
17 sion shall publish the application and pro-  
18 vide an opportunity for public comment on  
19 the compliance guidelines proposed in such  
20 application.

21 (ii) APPROVAL CRITERIA.—The Com-  
22 mission shall approve an application sub-  
23 mitted under paragraph (1), including the  
24 independent organization the application  
25 proposed to administer the compliance

1 guidelines proposed in such application, if  
2 the applicant demonstrates that the com-  
3 pliance guidelines—

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

6 (II) will provide for the regular  
7 review and validation by the inde-  
8 pendent organization to ensure that  
9 the covered entity continues to meet  
10 or exceed the requirements of this  
11 Act; and

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

21 (iii) **TIMELINE.**—Not later than 1  
22 year after receiving an application under  
23 paragraph (1), the Commission shall issue  
24 a determination approving or denying the  
25 application, including the independent or-

1 organization the application proposed to ad-  
2 minister the compliance guidelines pro-  
3 posed in such application, and providing an  
4 explanation for such approval or denial.

5 (B) APPROVAL OF MODIFICATIONS.—

6 (i) IN GENERAL.—If the independent  
7 organization administering a set of compli-  
8 ance guidelines makes any material change  
9 to guidelines previously approved by the  
10 Commission, the independent organization  
11 shall submit the updated compliance guide-  
12 lines to the Commission for approval. As  
13 soon as feasible, the Commission shall pub-  
14 lish the updated compliance guidelines and  
15 provide an opportunity for public comment.

16 (ii) TIMELINE.—Not later than 1 year  
17 after receiving the updated compliance  
18 guidelines under clause (i), the Commis-  
19 sion shall issue a determination approving  
20 or denying the material change to such  
21 guidelines.

22 (b) WITHDRAWAL OF APPROVAL.—

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

1 the requirements of this Act or a regulation promul-  
2 gated under this Act, or that compliance with any  
3 such approved guidelines is insufficiently enforced by  
4 the independent organization administering the  
5 guidelines, the Commission shall notify the relevant  
6 covered entity and independent organization of the  
7 Commission's determination to withdraw approval of  
8 such guidelines, including the basis for such deter-  
9 mination.

10 (2) OPPORTUNITY TO CURE.—

11 (A) IN GENERAL.—Not later than 180  
12 days after receiving notice from the Commission  
13 under paragraph (1), a covered entity and inde-  
14 pendent organization may cure any alleged defi-  
15 ciency with the compliance guidelines or the en-  
16 forcement thereof and submit each proposed  
17 cure to the Commission.

18 (B) EFFECT ON WITHDRAWAL OF AP-  
19 PROVAL.—If the Commission determines that  
20 the proposed cures described in subparagraph  
21 (A) eliminate the alleged deficiency in the com-  
22 pliance guidelines, then the Commission may  
23 not withdraw approval of such guidelines on the  
24 basis of such determination.



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

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

7 (2) as part of such self-certification, indicate  
8 the independent organization responsible for assess-  
9 ing compliance with such compliance guidelines.

10 (d) REBUTTABLE PRESUMPTION OF COMPLIANCE.—  
11 A covered entity with compliance guidelines approved by  
12 the Commission under this section, and that is in compli-  
13 ance with such guidelines, shall be entitled to a rebuttable  
14 presumption that such entity is in compliance with the rel-  
15 evant provisions of this Act if such covered entity is in  
16 compliance with such guidelines.

17 **SEC. 16. PRIVACY-ENHANCING TECHNOLOGY PILOT PRO-**  
18 **GRAM.**

19 (a) IN GENERAL.—Not later than 1 year after the  
20 date of enactment of this Act, the Commission shall estab-  
21 lish and carry out a pilot program to encourage private  
22 sector use of privacy-enhancing technology for the purpose  
23 of protecting covered data in compliance with section 9.

24 (b) COVERED ENTITY PARTICIPATION.—

1           (1) APPLICATION PROCESS.—A covered entity  
2 seeking to participate in the pilot program estab-  
3 lished under subsection (a) shall submit to the Com-  
4 mission, in such time, form, and manner as the  
5 Commission may require, an application that dem-  
6 onstrates the ability of the covered entity to use pri-  
7 vacy-enhancing technology to establish data security  
8 practices that meet or exceed the requirements of  
9 section 9.

10           (2) LIMITATIONS ON LIABILITY.—Any covered  
11 entity selected by the Commission to participate in  
12 the pilot program shall—

13           (A) with respect to any action under sec-  
14 tion 17 or 18 for a violation of section 9, be  
15 deemed to be in compliance with section 9 with  
16 respect to any covered data subject to the pri-  
17 vacy-enhancing technology; and

18           (B) for any action under section 19 alleg-  
19 ing a data breach due to a violation of section  
20 9, be entitled to a rebuttable presumption that  
21 such covered entity is in compliance with the  
22 relevant requirements under section 9 with re-  
23 spect to any covered data subject to the pri-  
24 vacy-enhancing technology.

25           (3) AUDIT OF COVERED ENTITIES.—

1 (A) IN GENERAL.—The Commission shall,  
2 on an ongoing basis, audit each covered entity  
3 participating in the pilot program to determine  
4 whether the covered entity is maintaining the  
5 use and implementation of privacy-enhancing  
6 technology to secure covered data.

7 (B) REMOVAL.—

8 (i) IN GENERAL.—If at any time the  
9 Commission determines that a covered en-  
10 tity participating in the pilot program is no  
11 longer maintaining the use and implemen-  
12 tation of privacy-enhancing technology, the  
13 Commission shall—

14 (I) notify the covered entity of  
15 such determination; and

16 (II) subject to clause (ii), remove  
17 such covered entity from participation  
18 in the pilot program, including the  
19 limitations on liability described in  
20 paragraph (2) that are afforded to  
21 participants.

22 (ii) OPPORTUNITY TO CURE.—Not  
23 later than 180 days after receiving notice  
24 from the Commission under clause (i), a  
25 covered entity may cure any alleged defi-

1                   ciency with its use and implementation of  
2                   privacy-enhancing technology and submit  
3                   to the Commission such proposed cure. If  
4                   the Commission determines that such cure  
5                   eliminates the alleged deficiency, then the  
6                   Commission may not remove the covered  
7                   entity from participation in the pilot pro-  
8                   gram.

9           (c) COORDINATION.—In carrying out the pilot pro-  
10 gram under subsection (a), the Commission shall—

11                   (1) solicit input from private, public, and aca-  
12                   demic stakeholders; and

13                   (2) in consultation with the Secretary of Com-  
14                   merce, develop ongoing public and private sector en-  
15                   gagement to disseminate voluntary, consensus-based  
16                   resources to increase the integration of privacy-en-  
17                   hancing technology in data collection, sharing, and  
18                   analytics by the public and private sectors.

19           (d) GAO STUDY AND REPORT.—

20                   (1) STUDY.—Not later than 3 years after the  
21                   date of enactment of this Act, the Comptroller Gen-  
22                   eral of the United States (in this subsection referred  
23                   to as the “Comptroller General”) shall conduct a  
24                   study to—

1 (A) assess the progress of the pilot pro-  
2 gram established under subsection (a);

3 (B) evaluate the Commission's use of pri-  
4 vacy-enhancing technology to support oversight  
5 of covered entities' data security practices; and

6 (C) develop recommendations to improve  
7 and advance privacy-enhancing technology, in-  
8 cluding by improving communication and co-  
9 ordination between covered entities and the  
10 Commission to increase use and implementation  
11 of privacy-enhancing technology by such entities  
12 and the Commission.

13 (2) INITIAL BRIEFING.—Not later than 1 year  
14 after the date of the enactment of this Act, the  
15 Comptroller General shall brief the Committee on  
16 Commerce, Science, and Transportation of the Sen-  
17 ate and the Committee on Energy and Commerce of  
18 the House of Representatives on the initial results of  
19 the study conducted under paragraph (1).

20 (3) FINAL REPORT.—Not later than 240 days  
21 after the initial briefing under paragraph (2), the  
22 Comptroller General shall submit to the Committee  
23 on Commerce, Science, and Transportation of the  
24 Senate and the Committee on Energy and Com-  
25 merce of the House of Representatives a final report

1 describing the results of the study conducted under  
2 paragraph (1), including the recommendations devel-  
3 oped under subparagraph (C) of such paragraph.

4 (e) SUNSET.—The Commission shall terminate the  
5 pilot program established under subsection (a) not later  
6 than 10 years after the date on which the pilot program  
7 is established.

8 (f) PRIVACY-ENHANCING TECHNOLOGY DEFINED.—  
9 The term “privacy-enhancing technology”—

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

15 (2) includes other technologies with  
16 functionality similar to homomorphic encryption, dif-  
17 ferential privacy, zero-knowledge proofs, synthetic  
18 data generation, federated learning, and secure  
19 multi-party computation.

20 **SEC. 17. ENFORCEMENT BY THE FEDERAL TRADE COMMIS-**  
21 **SION.**

22 (a) NEW BUREAU.—

23 (1) IN GENERAL.—The Commission shall estab-  
24 lish within the Commission a new bureau com-  
25 parable in structure, size, organization, and author-

1           ity to the existing bureaus within the Commission  
2           related to consumer protection and competition.

3           (2) MISSION.—The mission of the bureau es-  
4           tablished under this subsection shall be to assist the  
5           Commission in exercising the Commission’s author-  
6           ity under this Act and related authorities.

7           (3) TIMELINE.—The bureau shall be estab-  
8           lished, staffed, and fully operational not later than  
9           1 year after the date of enactment of this Act.

10          (b) ENFORCEMENT BY THE FEDERAL TRADE COM-  
11          MISSION.—

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

19           (2) POWERS OF THE COMMISSION.—

20           (A) IN GENERAL.—Except as provided in  
21           paragraphs (3) and (4) or otherwise provided in  
22           this Act, the Commission shall enforce this Act  
23           and the regulations promulgated under this Act  
24           in the same manner, by the same means, and  
25           with the same jurisdiction, powers, and duties

1 as though all applicable terms and provisions of  
2 the Federal Trade Commission Act (15 U.S.C.  
3 41 et seq.) were incorporated into and made a  
4 part of this Act.

5 (B) PRIVILEGES AND IMMUNITIES.—Any  
6 entity that violates this Act or a regulation pro-  
7 mulgated under this Act shall be subject to the  
8 penalties and entitled to the privileges and im-  
9 munities provided in the Federal Trade Com-  
10 mission Act (15 U.S.C. 41 et seq.).

11 (3) COMMON CARRIERS AND NONPROFITS.—  
12 Notwithstanding section (4), (5)(a)(2), or 6 of the  
13 Federal Trade Commission Act (15 U.S.C. 44,  
14 45(a)(2), 46) or any jurisdictional limitation of the  
15 Commission, the Commission shall also enforce this  
16 Act and the regulations promulgated under this Act  
17 in the same manner provided in paragraphs (1) and  
18 (2), with respect to—

19 (A) common carriers subject to title II of  
20 the Communications Act of 1934 (47 U.S.C.  
21 201–231) as currently enacted or subsequently  
22 amended; an

23 (B) organizations not organized to carry  
24 on business for their own profit or that of their  
25 members.



1           (4) PRIVACY AND SECURITY VICTIMS RELIEF  
2           FUND.—

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

8           (B) DEPOSITS.—

9           (i) DEPOSITS FROM THE COMMIS-  
10          SION.—The Commission shall deposit into  
11          the Victims Relief Fund the amount of any  
12          civil penalty obtained against any entity in  
13          any judicial or administrative action the  
14          Commission commences to enforce this Act  
15          or a regulation promulgated under this  
16          Act.

17          (ii) DEPOSITS FROM THE ATTORNEY  
18          GENERAL OF THE UNITED STATES.—The  
19          Attorney General of the United States  
20          shall deposit into the Victims Relief Fund  
21          the amount of any civil penalty obtained  
22          against any entity in any judicial or ad-  
23          ministrative action the Attorney General  
24          commences on behalf of the Commission to

1 enforce this Act or a regulation promul-  
2 gated under this Act.

3 (C) USE OF FUND AMOUNTS.—

4 (i) AVAILABILITY TO THE COMMISS-  
5 SION.—Notwithstanding section 3302 of  
6 title 31, United States Code, amounts in  
7 the Victims Relief Fund shall be available  
8 to the Commission, without fiscal year lim-  
9 itation, to provide redress, payments or  
10 compensation, or other monetary relief to  
11 persons affected by an act or practice for  
12 which civil penalties have been obtained  
13 under this Act.

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

20 (I) consumer or business edu-  
21 cation relating to privacy and data se-  
22 curity; or

23 (II) engaging in technological re-  
24 search that the Commission considers  
25 necessary to enforce this Act.

1 (D) CALCULATION.—

2 (i) PENALTY OFFSET FOR STATE OR  
3 INDIVIDUAL ACTIONS.—Any amount that a  
4 court orders an entity to pay under this  
5 subsection shall be offset by any amount  
6 the person received from an action brought  
7 against the entity for the same violation  
8 under section 18 or 19.

9 (ii) RELIEF OFFSET FOR STATE OR  
10 INDIVIDUAL ACTIONS.—Any amount that  
11 the Commission provides to a person as re-  
12 dress, payments or compensation, or other  
13 monetary relief under subparagraph (C)  
14 shall be offset by any amount the person  
15 received from an action brought against  
16 the entity for the same violation under sec-  
17 tion 18 or 19.

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

25 (c) REPORT.—

1           (1) IN GENERAL.—Not later than 4 years after  
2           the date of the enactment of this Act, and annually  
3           thereafter, the Commission shall, submit to Congress  
4           a report on investigations conducted for alleged vio-  
5           lations this Act, including—

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

8                   (B) the number of such investigations the  
9           Commission has closed with no official agency  
10          action;

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

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

18           (2) PRIVACY PROTECTIONS.—The report re-  
19          quired under paragraph (1) shall not include the  
20          identity of the person who is the subject of the in-  
21          vestigation or any other information that identifies  
22          such person.

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

1 Congress a plan for the next calendar year describ-  
2 ing the projected activities of the Commission under  
3 this Act, including each of the following:

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

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

10 (C) Any plans to develop, update, or with-  
11 draw guidance required under this Act.

12 (D) Any plans to restructure the Commis-  
13 sion or establish, alter, or terminate working  
14 groups.

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

19 **SEC. 18. ENFORCEMENT BY STATES.**

20 (a) CIVIL ACTION.—

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

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

11                   (A) enjoin that act or practice;

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

14                   (C) obtain civil penalties;

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

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

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

22           (2) LIMITATION.—In any case where the attor-  
23      ney general of a State, the chief consumer protection  
24      officer of a State, or an officer of office of the State  
25      authorized to enforce privacy or data security laws

1 applicable to covered entities or service providers  
2 brings an action under paragraph (1), no other offi-  
3 cer of the same State may institute a civil action  
4 under paragraph (1) against the same defendant for  
5 the same violation of this Act or a regulation pro-  
6 mulgated under this Act.

7 (b) RIGHTS OF THE COMMISSION.—

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

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

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

19 (2) NOTIFICATION TIMELINE.—Where it is not  
20 feasible for the State officer to provide the notifica-  
21 tion required by paragraph (1) before initiating a  
22 civil action under subsection (a), the State officer  
23 shall notify the Commission immediately after initi-  
24 ating the civil action.

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

12           (d) INVESTIGATORY POWERS.—Nothing in this sec-  
13 tion shall be construed to prevent the attorney general of  
14 a State, the chief consumer protection officer of a State,  
15 or an officer or office of a State authorized to enforce pri-  
16 vacy or data security laws applicable to covered entities  
17 or service providers from exercising the powers conferred  
18 on such officer or office to conduct investigations, to ad-  
19 minister oaths or affirmations, or to compel the attend-  
20 ance of witnesses or the production of documentary or  
21 other evidence.

22           (e) VENUE; SERVICE OF PROCESS.—

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



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

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

6            (A) is an inhabitant; or

7            (B) may be found.

8        (f) GAO STUDY.—Not later than 1 year after the  
9        date of enactment of this Act, the Comptroller General  
10       of the United States shall conduct a study on State attor-  
11       neys general’s hiring of, or otherwise contracting with,  
12       outside firms to assist in the enforcement of this Act. The  
13       study shall include—

14            (1) the frequency of such hires;

15            (2) the contingency fees or hourly rates and  
16        other costs of hiring or contracting with outside  
17        firms;

18            (3) the types of matters outside firms are hired  
19        or contracted with for;

20            (4) the bid process for such outside law firm  
21        work and selection process, including reviews of con-  
22        flicts of interest;

23            (5) the practices State attorneys general set in  
24        place to protect sensitive information that would be-

1       come accessible by outside firms while they are as-  
2       sisting in enforcement efforts;

3               (6) the percent of monetary recovery that is re-  
4       turned to victims and the percent that is retained by  
5       the law firm; and

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

8       (g) CALCULATION.—Any amount that a court orders  
9       an entity to pay in an action brought under subsection  
10      (a) shall be offset by any amount the person received from  
11      an action brought against the entity for the same violation  
12      under section 17 or 19.

13      (h) PRESERVATION OF STATE POWERS.—Except as  
14      provided in subsection (c), no provision of this section  
15      shall be construed as altering, limiting, or affecting the  
16      authority of a State attorney general, the chief consumer  
17      protection officer of a State, or an officer or office of a  
18      State authorized to enforce laws applicable to covered enti-  
19      ties or service providers to—

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

23               (2) exercise the powers conferred on the attor-  
24      ney general, the chief consumer protection officer of  
25      a State, or such officer or office by the laws of the

1 State, including the ability to conduct investigations,  
2 to administer oaths or affirmations, or to compel the  
3 attendance of witnesses or the production of docu-  
4 mentary or other evidence.

5 **SEC. 19. ENFORCEMENT BY INDIVIDUALS.**

6 (a) ENFORCEMENT BY INDIVIDUALS.—

7 (1) IN GENERAL.—Subject to subsections (b)  
8 and (c), an individual may bring a civil action  
9 against an entity for a violation of subsections (b)  
10 or (c) of section 3, subsections (a) or (e) of section  
11 4, section 5, subsections (a) or (b)(2) of section 6,  
12 section 7, section 8, section 9 to the extent such  
13 claim alleges a data breach arising from a violation  
14 of subsection (a) of such section, subsection (d) of  
15 section 11, subsection (c)(4) of section 12, sub-  
16 section (a) of section 13, section 14, or a regulation  
17 promulgated thereunder, in an appropriate Federal  
18 district court of the United States.

19 (2) RELIEF.—

20 (A) IN GENERAL.—In a civil action  
21 brought under paragraph (1) in which the  
22 plaintiff prevails, the court may award the  
23 plaintiff—

24 (i) an amount equal to the sum of any  
25 actual damages;

1 (ii) injunctive relief, including an  
2 order that the entity retrieve any covered  
3 data transferred in violation of this Act;

4 (iii) declaratory relief; and

5 (iv) reasonable attorney's fees and liti-  
6 gation costs.

7 (B) BIOMETRIC AND GENETIC INFORMA-  
8 TION.—In a civil action brought under para-  
9 graph (1) for a violation of this Act with re-  
10 spect to section 3(c) where the conduct under-  
11 lying the violation occurred primarily and sub-  
12 stantially in Illinois, in which the plaintiff pre-  
13 vails, the court may award the plaintiff—

14 (i) the same relief as set forth in sec-  
15 tion 20 of the Biometric Information Pri-  
16 vacy Act (740 ILCS 14/20), as such stat-  
17 ute read on January 1, 2024; or

18 (ii) the same relief as set forth in sec-  
19 tion 40 of the Genetic Information Privacy  
20 Act (740 ILCS 513/40), as such statute  
21 read on January 1, 2024.

22 (C) DATA SECURITY.—

23 (i) IN GENERAL.—In a civil action  
24 brought under paragraph (1) for a viola-  
25 tion of section 9, alleging unauthorized ac-



1 the sensitive covered data are not  
2 encrypted or redacted:

3 (aa) A government identifier  
4 as described in section  
5 2(34)(A)(i).

6 (bb) Any sensitive covered  
7 data described in section  
8 2(34)(A)(iv).

9 (cc) Health information, but  
10 only to the extent that such in-  
11 formation reveals the individual's  
12 history of medical treatment or  
13 diagnosis by a health care profes-  
14 sional.

15 (dd) Biometric information.

16 (ee) Genetic information.

17 (D) LIMITATIONS ON DUAL ACTIONS.—

18 Any amount that a court orders an entity to  
19 pay to an individual under subparagraph (A)(i),  
20 (B), or (C) shall be offset by any amount the  
21 individual received from an action brought  
22 against the entity for the same violation under  
23 section 17 or 18.

24 (b) OPPORTUNITY TO CURE IN ACTIONS FOR IN-  
25 JUNCTIVE RELIEF.—

1           (1) NOTICE.—Subject to paragraph (3), an ac-  
2           tion for injunctive relief may be brought by an indi-  
3           vidual under this section only if, prior to initiating  
4           such action against an entity, the individual provides  
5           to the entity 30 days’ written notice identifying the  
6           specific provisions of this Act the individual alleges  
7           have been or are being violated.

8           (2) EFFECT OF CURE.—In the event a cure is  
9           possible, if, within the 30-day period, the entity  
10          cures the noticed violation and provides the indi-  
11          vidual with an express written statement that the  
12          violation has been cured and that no such further  
13          violation shall occur, an action for injunctive relief  
14          shall not be permitted.

15          (3) SUBSTANTIAL PRIVACY HARM.—Notice shall  
16          not be required under paragraph (1) prior to filing  
17          an action for injunctive relief for a violation of this  
18          Act that resulted in a substantial privacy harm.

19          (c) NOTICE OF ACTIONS SEEKING ACTUAL DAM-  
20          AGES.—

21          (1) NOTICE.—Subject to paragraph (2), an ac-  
22          tion for actual damages may be brought by an indi-  
23          vidual under this section only if, prior to initiating  
24          such action against an entity, the individuals pro-  
25          vides to the entity 30 days’ written notice identifying

1 the specific provisions of this Act the individual al-  
2 leges have been or are being violated.

3 (2) SUBSTANTIAL PRIVACY HARM.—Notice shall  
4 not be required under paragraph (1) prior to filing  
5 an action for actual damages for a violation of this  
6 Act that resulted in a substantial privacy harm if  
7 such action includes a claim for a preliminary in-  
8 junction or temporary restraining order.

9 (d) PREDISPUTE ARBITRATION AGREEMENTS.—

10 (1) IN GENERAL.—Notwithstanding any other  
11 provision of law, at the election of the individual al-  
12 leging a violation of this Act, no pre-dispute arbitra-  
13 tion agreement shall be valid or enforceable with re-  
14 spect to—

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

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

19 (2) DETERMINATION OF APPLICABILITY.—Any  
20 issue as to whether this section applies to a dispute  
21 shall be determined under Federal law. The applica-  
22 bility of this section to an agreement to arbitrate  
23 and the validity and enforceability of an agreement  
24 to which this section applies shall be determined by  
25 a Federal court, rather than an arbitrator, irrespec-





1 (B) expressly preempt laws of a State or  
2 political subdivision thereof, as provided in this  
3 subsection.

4 (2) IN GENERAL.—Except as provided in para-  
5 graph (3), no State or political subdivision thereof  
6 may adopt, maintain, enforce, or continue in effect  
7 any law, regulation, rule, or requirement covered by  
8 the provisions of this Act or a rule, regulation, or re-  
9 quirement promulgated under this Act.

10 (3) STATE LAW PRESERVATION.—Paragraph  
11 (1) shall not be construed to preempt, displace, or  
12 supplant the following State laws, rules, regulations,  
13 or requirements:

14 (A) Consumer protection laws of general  
15 applicability, such as laws regulating deceptive,  
16 unfair, or unconscionable practices.

17 (B) Civil rights laws.

18 (C) Provisions of laws that address the pri-  
19 vacy rights or other protections of employees or  
20 employee information.

21 (D) Provisions of laws that address the  
22 privacy rights or other protections of students  
23 or student information.

24 (E) Provision of laws that address notifica-  
25 tion requirements in the event of a data breach.

1 (F) Contract or tort law.

2 (G) Criminal laws unrelated to data pri-  
3 vacy or data security.

4 (H) Criminal or civil laws regarding—

5 (i) blackmail;

6 (ii) stalking, including cyberstalking;

7 (iii) cyberbullying;

8 (iv) intimate images, including au-  
9 thentic or generated by a computer or by  
10 artificial intelligence, known to be non-  
11 consensual;

12 (v) child abuse;

13 (vi) child sexual abuse material;

14 (vii) child abduction or attempted  
15 child abduction;

16 (viii) child trafficking; or

17 (ix) sexual harassment.

18 (I) Public safety or sector specific laws un-  
19 related to data privacy or data security, pro-  
20 vided that such laws do not directly conflict  
21 with the provisions of this Act.

22 (J) Provisions of laws that address public  
23 records, criminal justice information systems,  
24 arrest records, mug shots, conviction records, or  
25 non-conviction records.

1           (K) Provisions of laws that address bank-  
2           ing records, financial records, tax records, so-  
3           cial security numbers, credit cards, identity  
4           theft, credit reporting and investigations, credit  
5           repair, credit clinics, or check-cashing services.

6           (L) Provisions of laws that address elec-  
7           tronic surveillance, wiretapping, telephone mon-  
8           itoring.

9           (M) Provisions of laws that address unso-  
10          solicited email messages, telephone solicitation, or  
11          caller ID.

12          (N) Provisions of laws that protect the pri-  
13          vacy of health information, healthcare informa-  
14          tion, medical information, medical records, HIV  
15          status, or HIV testing.

16          (O) Provisions of laws that address the  
17          confidentiality of library records.

18          (P) Provisions of laws that address the use  
19          of encryption as a means of providing data se-  
20          curity.

21       (b) FEDERAL LAW PRESERVATION.—

22           (1) IN GENERAL.—Nothing in this Act or a reg-  
23          ulation promulgated under this Act may be con-  
24          strued to limit—

1 (A) the authority of the Commission, or  
2 any other Executive agency, under any other  
3 provision of law;

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

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

11 (2) ANTITRUST SAVINGS CLAUSE.—

12 (A) DEFINITION OF ANTITRUST LAWS.—  
13 For the purposes of this paragraph, the term  
14 “antitrust laws”—

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

18 (ii) includes section 5 of the Federal  
19 Trade Commission Act (15 U.S.C. 45), to  
20 the extent that section applies to unfair  
21 methods of competition.

22 (B) RULE OF CONSTRUCTION.—Nothing in  
23 this Act, or the regulatory regime created under  
24 this Act, may be construed to modify, impair,



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

5 (v) The requirements regarding the  
6 confidentiality of substance use disorder  
7 information under section 543 of the Pub-  
8 lic Health Service Act (42 U.S.C. 290dd–  
9 2) or any regulation promulgated there-  
10 under.

11 (vi) The Fair Credit Reporting Act  
12 (15 U.S.C. 1681 et seq.).

13 (vii) Section 444 of the General Edu-  
14 cation Provisions Act of 1974 (commonly  
15 known as the “Family Educational Rights  
16 and Privacy Act”) (20 U.S.C. 1232g) and  
17 part 99 of title 34, Code of Federal Regu-  
18 lations (or any successor regulation), to  
19 the extent such covered entity or service  
20 provider is an educational agency or insti-  
21 tution as defined in such section of such  
22 Act or section 99.3 of title 34, Code of  
23 Federal Regulations (or any successor reg-  
24 ulation).

1 (C) IMPLEMENTATION GUIDANCE.—Not  
2 later than 1 year after the date of enactment of  
3 this Act, the Commission shall issue guidance  
4 regarding the implementation of this para-  
5 graph.

6 (4) APPLICATION OF OTHER FEDERAL DATA  
7 SECURITY REQUIREMENTS.—

8 (A) IN GENERAL.—A covered entity or  
9 service provider that is required to comply with  
10 the laws and regulations described in subpara-  
11 graph (B) and is in compliance with the infor-  
12 mation security requirements of such laws and  
13 regulations shall be deemed to be in compliance  
14 with section 9 of this Act, solely and exclusively  
15 with respect to any data subject to the require-  
16 ments of such laws and regulations.

17 (B) LAWS AND REGULATIONS DE-  
18 SCRIBED.—For purposes of subparagraph (A),  
19 the laws and regulations described in this sub-  
20 paragraph are the following:

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

23 (ii) The Health Information Tech-  
24 nology for Economic and Clinical Health  
25 Act (42 U.S.C. 17931 et seq.).



1 (iii) Part C of title XI of the Social  
2 Security Act (42 U.S.C. 1320d et seq.).

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

7 (C) IMPLEMENTATION GUIDANCE.—Not  
8 later than 1 year after the date of enactment of  
9 this Act, the Commission shall issue guidance  
10 regarding the implementation of this para-  
11 graph.

12 (c) PRESERVATION OF COMMON LAW OR STATUTORY  
13 CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this  
14 Act nor any amendment, standard, rule, requirement, as-  
15 sessment, law, or regulation promulgated under this Act  
16 shall be construed to preempt, displace, or supplant any  
17 Federal or State common law right or remedy, or any stat-  
18 ute creating a remedy for civil relief, including any cause  
19 of action for personal injury, wrongful death, property  
20 damage, or other financial, physical, reputational, or psy-  
21 chological injury based in negligence, strict liability, prod-  
22 ucts liability, failure to warn, or an objectively offensive  
23 intrusion into the private affairs or concerns of the indi-  
24 vidual, or any other legal theory of liability under any Fed-  
25 eral or State common law, or any State statutory law, ex-

1 cept that a violation of this Act or a regulation promul-  
2 gated under this Act may not be pleaded as an element  
3 of any violation of such law.

4 (d) NON-APPLICATION OF CERTAIN PROVISIONS OF  
5 THE COMMUNICATIONS ACT OF 1934.—

6 (1) IN GENERAL.—Notwithstanding any other  
7 provision of law, and except as provided in para-  
8 graph (2), the Communications Act of 1934 (47  
9 U.S.C. 151 et seq.) and all Acts amendatory thereof  
10 or supplementary thereto and any regulation pro-  
11 mulgated by the Federal Communications Commis-  
12 sion under such an Act shall not apply to any cov-  
13 ered entity or service provider with respect to the  
14 collection, processing, retention, transfer, or security  
15 of covered data to the extent that such collection,  
16 processing, retention, transfer, or security of covered  
17 data is governed by the requirements of this Act.

18 (2) EXCEPTIONS.—Paragraph (1) shall not pre-  
19 clude the application of any of the following to a  
20 covered entity or service provider with respect to the  
21 collection, processing, retention, transfer, or security  
22 of covered data:

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

1 (B) Section 64.2011 of title 47, Code of  
2 Federal Regulations (or any successor regula-  
3 tion).

4 (C) Mitigation measures and actions taken  
5 pursuant to Executive Order 13913 (85 Fed.  
6 Reg. 19643; relating to the establishment of the  
7 Committee for the Assessment of Foreign Par-  
8 ticipation in the United States Telecommuni-  
9 cations Services Sector).

10 (D) Any obligation under an international  
11 treaty related to the exchange of traffic imple-  
12 mented and enforced by the Federal Commu-  
13 nications Commission.

14 **SEC. 21. CHILDREN'S ONLINE PRIVACY PROTECTION ACT**  
15 **OF 1998.**

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

20 **SEC. 22. TERMINATION OF FTC RULEMAKING ON COMMER-**  
21 **CIAL SURVEILLANCE AND DATA SECURITY.**

22 Beginning on the date of enactment of this Act, the  
23 Commission's Trade Regulation Rule on Commercial Sur-  
24 veillance and Data Security proposed rulemaking, as pub-  
25 lished on August, 8, 2022, shall be terminated.

1 **SEC. 23. SEVERABILITY.**

2       If any provision of this Act, or the application thereof  
3 to any person or circumstance, is held to be invalid, the  
4 remainder of this Act, and the application of such provi-  
5 sion to other persons not similarly situated or to other  
6 circumstances, shall not be affected.

7 **SEC. 24. EFFECTIVE DATE.**

8       This Act shall take effect on the date that is 180 days  
9 after the date of enactment of the Act, unless otherwise  
10 specified in this Act.