

[DISCUSSION DRAFT]

118TH CONGRESS
2D SESSION

H. R. _____

To [_____] , and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M. _____ introduced the following bill; which was referred to the
Committee on _____

A BILL

To [_____] , and for other purposes.

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

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

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

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

- Sec. 1. Short title; table of contents.
- 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 Federal Trade Commission.
- Sec. 18. Enforcement by States.
- Sec. 19. Enforcement by persons.
- Sec. 20. Relation to other laws.
- Sec. 21. Childrens 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 author-
8 ization of the individual for an act or prac-
9 tice;

10 (ii) is provided in response to a spe-
11 cific request from a covered entity, or a
12 service provider on behalf of a covered en-
13 tity; and

14 (iii) that meets the requirements of
15 subparagraph (B).

16 (B) **REQUEST REQUIREMENTS.**—The re-
17 quirements of this subparagraph with respect to

1 a request made under subparagraph (A) are the
2 following:

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

6 (ii) The request includes a description
7 of each act or practice for which the con-
8 sent of such individual is sought and—

9 (I) clearly distinguishes between
10 an act or practice that is necessary to
11 fulfill a request of the individual and
12 an act or practice that is for another
13 purpose;

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

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

1 (iii) The request clearly explains the
2 applicable rights of the individual related
3 to consent.

4 (iv) The request is made in a manner
5 reasonably accessible to and usable by indi-
6 viduals living with disabilities.

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

11 (vi) The option to refuse consent is at
12 least as prominent as the option to provide
13 consent, and the option to refuse consent
14 takes the same number of steps or fewer
15 as the option to provide consent.

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

21 (2) BIOMETRIC INFORMATION.—

22 (A) IN GENERAL.—The term “biometric
23 information” means any covered data that is
24 specific to an individual and is generated from
25 the measurement or processing of the unique

1 biological, physical, or physiological characteris-
2 tics of the individual and that is linked or rea-
3 sonably linkable to the individual, including—

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

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

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

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

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

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

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

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

10 (A) ownership of, or the power to vote,
11 more than 50 percent of the outstanding shares
12 of any class of voting security of the entity;

13 (B) control over the election of a majority
14 of the directors of the entity (or of individuals
15 exercising similar functions); or

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

18 (8) COVERED ALGORITHM.—The term “covered
19 algorithm” means a computational process, includ-
20 ing a process derived from machine learning, statis-
21 tics, or other data processing or artificial intelligence
22 techniques, that makes a decision or facilitates
23 human decision-making by using covered data, which
24 included determining the provision of products or
25 services or ranking, ordering, promoting, recom-

1 mending, amplifying, or similarly determining the
2 delivery or display of information to an individual.

3 (9) COVERED DATA.—

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

10 (B) EXCLUSIONS.—The term “covered
11 data” does not include—

12 (i) de-identified data;

13 (ii) employee information;

14 (iii) publicly available information;

15 (iv) inferences made exclusively from
16 multiple independent sources of publicly
17 available information if such inferences—

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

22 (II) are not combined with cov-
23 ered data; or

1 (v) information in the collection of a
2 library, archive, or museum if the library,
3 archive, or museum has—

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

8 (II) a public service mission;

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

13 (IV) collections composed of law-
14 fully acquired materials with respect
15 to which all licensing conditions are
16 met.

17 (10) COVERED ENTITY.—

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

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

1 (ii) is a common carrier subject to
2 title II of the Communications Act of 1934
3 (47 U.S.C. 201 201–231); or

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

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

12 (C) EXCLUSION.—The term “covered enti-
13 ty” does not include—

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

20 (ii) an entity that is collecting, proc-
21 essing, retaining, or transferring covered
22 data on behalf of a Federal, State, Tribal,
23 or local government entity, to the extent
24 that such entity is acting as a service pro-
25 vider to the government entity;

1 (iii) a small business;

2 (iv) the National Center for Missing
3 and Exploited Children; or

4 (v) except with respect to require-
5 ments under section 9, a nonprofit organi-
6 zation whose primary mission is to prevent,
7 investigate, or deter fraud or to train anti-
8 fraud professionals, or educate the public
9 about fraud, including insurance fraud, se-
10 curities fraud, and financial fraud, to the
11 extent the organization collects, processes,
12 retains, or transfers covered data in fur-
13 therance of such primary mission.

14 (D) NONAPPLICATION TO SERVICE PRO-
15 VIDERS.—An entity shall not be considered to
16 be a “covered entity” for the purposes of this
17 Act, insofar as the entity is acting as a service
18 provider.

19 (11) COVERED HIGH-IMPACT SOCIAL MEDIA
20 COMPANY.—The term “covered high-impact social
21 media company” means a covered entity that pro-
22 vides any internet-accessible platform that—

23 (A) generates \$3,000,000,000 or more in
24 global annual revenue, including the revenue

1 generated by any affiliate of such covered enti-
2 ty;

3 (B) has 300,000,000 or more global
4 monthly active users for not fewer than 3 of the
5 preceding 12 months on the platform of such
6 covered entity; and

7 (C) constitutes an online product or service
8 that is primarily used by users to access or
9 share user-generated content.

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

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

16 (14) DATA BROKER.—

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

23 (B) PRINCIPAL SOURCE OF REVENUE.—
24 For purposes of this paragraph, the term “prin-

1 cipal source of revenue” means for the prior 12-
2 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 (15) DE-IDENTIFIED DATA.—

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

1 (i) takes reasonable physical, adminis-
2 trative, or technical measures to ensure
3 that the information cannot, at any point,
4 be used to re-identify any individual or de-
5 vice that identifies or is linked or reason-
6 ably linkable to an individual;

7 (ii) publicly commits in a clear and
8 conspicuous manner to—

9 (I) process, retain, or transfer
10 the information solely in a de-identi-
11 fied form without any reasonable
12 means for re-identification; and

13 (II) not attempt to re-identify the
14 information with any individual or de-
15 vice that identifies or is linked or rea-
16 sonably linkable to an individual; and

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

20 (I) comply with all of the provi-
21 sions of this paragraph/clauses (i) and
22 (ii)with respect to the information;
23 and

24 (II) require that such contractual
25 obligations be included contractually

1 in all subsequent instances for which
2 the data may be received.

3 (B) HEALTH INFORMATION.—The term
4 “de-identified data” includes health information
5 (as defined in section 262 of the Health Insur-
6 ance Portability and Accountability Act of 1996
7 (42 U.S.C. 1320d)) that has been de-identified
8 in accordance with section 164.514(b) of title
9 45, Code of Federal Regulations, provided that
10 if such information is subsequently provided to
11 an entity that is not an entity subject to parts
12 160 and 164 of such title 45, such entity must
13 comply with clauses (ii) and (iii) of subpara-
14 graph (A) for the information to be considered
15 de-identified under this Act.

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

22 (17) DEVICE.—The term “device” means any
23 electronic equipment capable of collecting, proc-
24 essing, retaining, or transferring covered data that is

1 used by 1 or more individuals, including a connected
2 device or a portable connected device.

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

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

15 (A) about an individual in the course of
16 employment or application for employment (in-
17 cluding on a contract or temporary basis), if
18 such data is retained or processed by the cov-
19 ered entity or service provider solely for pur-
20 poses necessary for the employment or applica-
21 tion of the individual;

22 (B) that is emergency contact information
23 for an individual who is an employee, or job ap-
24 plicant of the covered entity, if such data is re-
25 tained or processed by the covered entity or

1 service provider solely for the purpose of having
2 an emergency contact for such individual on
3 file; or

4 (C) about an individual (or a relative of an
5 individual) who is an employee or former em-
6 ployee of the covered entity for the purpose of
7 administering benefits to which such individual
8 or relative is entitled on the basis of the em-
9 ployment of the individual with the covered en-
10 tity, if such data is retained or processed by the
11 covered entity or service provider solely for the
12 purpose of administering such benefits.

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

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

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

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

1 the extracted deoxyribonucleic acid (DNA) of
2 an individual; or

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

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

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

16 (25) LARGE DATA HOLDER.—

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

23 (i) the covered data of—

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

1 (II) 15,000,000 portable con-
2 nected devices that identify or are
3 linked or reasonably linkable to 1 or
4 more individuals; and

5 (III) 35,000,000 connected de-
6 vices that identify or are linked or
7 reasonable linkable to 1 or more indi-
8 viduals; or

9 (ii) the sensitive covered data of—

10 (I) more than 200,000 individ-
11 uals;

12 (II) 300,000 portable connected
13 devices that identify or are linked or
14 reasonable linkable to 1 or more indi-
15 viduals; and

16 (III) 700,000 connected devices
17 that identify or are linked or reason-
18 ably linkable to 1 or more individuals.

19 (B) EXCLUSIONS.—For the purposes of
20 subparagraph (A), a covered entity or service
21 provider may not be considered a large data
22 holder solely on the basis of collecting, proc-
23 essing, retaining, or transferring to a service
24 provider—

1 (i) personal mailing or email address-
2 es;

3 (ii) personal telephone numbers;

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

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

18 (C) DEFINITION OF ANNUAL GROSS REV-
19 ENUE.—For the purposes of subparagraph (A)
20 in determining if any covered entity or service
21 provider is a large data holder, the term “an-
22 nual gross revenue”, with respect to any cov-
23 ered entity or service provider—

24 (i) means the gross receipts the cov-
25 ered entity or service provider received, in

1 whatever form from all sources, without
2 subtracting any costs or expenses; and

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

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

14 (A) integrated into any product or service;

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

17 (C) used for targeted advertising or to oth-
18 erwise market to any individual or device of an
19 individual.

20 (27) MATERIAL CHANGE.—The term “material
21 change” means a change by an entity with respect
22 to treatment of covered data that would likely affect
23 the decision of an individual to provide affirmative
24 express consent for, or opt out of, the collection,

1 processing, retention, or transfer of covered data
2 pertaining to such individual.

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

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

16 (ii) widely distributed media;

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

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

25 (B) CLARIFICATIONS; LIMITATIONS.—

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

8 (ii) BUSINESS CONTACT INFORMA-
9 TION.—The term “publicly available infor-
10 mation” includes business contact informa-
11 tion of an employee that is made available
12 on a website or online service made avail-
13 able to all members of the public, including
14 the name, position or title, business tele-
15 phone number, business email address , or
16 business address of the employee.

17 (iii) OTHER LIMITATIONS.—The term
18 “publicly available information” does not
19 include—

20 (I) any obscene visual depiction
21 (as such term is used in section 1460
22 of title 18, United States Code);

23 (II) derived data from publicly
24 available information that reveals in-
25 formation about an individual that

1 meets the definition of sensitive cov-
2 ered data;

3 (III) biometric information;

4 (IV) genetic information;

5 (V) covered data that has been
6 combined with publicly available infor-
7 mation; or

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

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

14 (34) SENSITIVE COVERED DATA.—

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

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

23 (ii) Any information that describes or
24 reveals the past, present, or future physical
25 health, mental health, disability, diagnosis,

1 or healthcare condition or treatment of an
2 individual.

3 (iii) Genetic information.

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

9 (v) Biometric information.

10 (vi) Precise geolocation information.

11 (vii) The private communications of
12 an individual (such as voicemails, emails,
13 texts, direct messages, or mail) or informa-
14 tion identifying the parties to such commu-
15 nications, information contained in tele-
16 phone bills, voice communications, and any
17 information that pertains to the trans-
18 mission of voice communications, including
19 numbers called, numbers from which calls
20 were placed, the time calls were made, call
21 duration, and location information of the
22 parties to the call, unless the covered enti-
23 ty is an intended recipient of the commu-
24 nication.

1 (viii) Account or device log-in creden-
2 tials.

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

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

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

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

1 ing any such data used solely for transfers
2 for independent video measurement).

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

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

16 (xv) Information revealing the online
17 activities of an individual over time and
18 across websites or online services that do
19 not share common branding, or over time
20 on any website or online service operated
21 by a high-impact social media company.

22 (xvi) Information about an individual
23 when the covered entity or service provider
24 has knowledge that the individual is a cov-
25 ered minor.

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

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

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

15 (i) is related by common ownership or
16 corporate control to the provider of broad-
17 cast television service, or streaming media
18 service; 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 with
6 respect to a specific collecting, processing,
7 retaining, or transferring of data, if the
8 entity, jointly or with others, determines
9 the purposes and means of the specific col-
10 lecting, processing, retaining, or transfer-
11 ring of data.

12 (ii) CONTEXT REQUIRED.—Whether
13 an entity is a covered entity or a service
14 provider depends on the facts surrounding,
15 and the context in which, the data is col-
16 lected, processed, retained, or transferred.

17 (36) SMALL BUSINESS.—

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

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

1 such period is less than 3years) did not ex-
2 ceed \$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 a purpose was de-
11 leted or de-identified within 90 days, un-
12 less necessary to investigate fraud or as
13 consistent with a return or warranty policy
14 of the entity; 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 its members, means the gross receipts the enti-
23 ty received, in whatever form from all sources,
24 without subtracting any costs or expenses, and
25 includes contributions, gifts, grants (except for

1 grants from the Federal Government), dues or
2 other assessments, income from investments, or
3 proceeds from the sale of real or personal prop-
4 erty.

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

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

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

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

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

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

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

3 (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 to a group of individuals or
8 devices identified by unique persistent identi-
9 fiers) an online advertisement that is selected
10 based on known or predicted preferences or in-
11 terests associated with the individual or a de-
12 vice identified by a unique identifier;

13 (B) does not include—

14 (i) advertising or marketing content to
15 an individual in response to the specific re-
16 quest of the individual for information or
17 feedback;

18 (ii) first-party advertising based on a
19 visit to or use, by an individual, of a
20 website or online service that offers a prod-
21 uct or service that is related to the subject
22 of the advertisement;

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.—

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

17 (B) EXCLUSION.—The term “unique per-
18 sistent identifier” does not include an identifier
19 assigned by a covered entity for the specific
20 purpose of giving effect to an individual’s exer-
21 cise of affirmative express consent or opt out by
22 an individual with respect to the collecting,
23 processing, retaining, and transfer of covered
24 data otherwise limiting the collecting, proc-

1 essing, retaining, or transfer of such informa-
2 tion.

3 (44) WIDELY DISTRIBUTED MEDIA.—

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

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

16 **SEC. 3. DATA MINIMIZATION.**

17 (a) IN GENERAL.—Subject to subsections (b) and (c),
18 a covered entity, or a service provider on behalf of a cov-
19 ered entity may not collect, process, retain, or transfer
20 covered data of an individual—

21 (1) beyond what is necessary, proportionate,
22 and limited—

23 (A) to provide or maintain—

24 (i) a specific product or service re-
25 quested by the individual to whom the data

1 pertains, including any associated routine
2 administrative, operational, or account-
3 servicing activity, such as billing, shipping,
4 delivery, storage, or accounting; or

5 (ii) a communication by the covered
6 entity to the individual reasonably antici-
7 pated within the context of the relationship
8 between the covered entity and the indi-
9 vidual; or

10 (B) for a purpose expressly permitted
11 under subsection (d); or

12 (2) for a purpose other than those expressly
13 permitted under subsection (d).

14 (b) SENSITIVE COVERED DATA.—

15 (1) IN GENERAL.—Unless for a purpose ex-
16 pressly permitted under subsection (d), a covered en-
17 tity, or a service provider on behalf of a covered en-
18 tity, may not transfer sensitive covered data to a
19 third party without the affirmative express consent
20 of the individual to whom such data pertains.

21 (2) WITHDRAWAL OF AFFIRMATIVE EXPRESS
22 CONSENT.—

23 (A) IN GENERAL.—A covered entity shall
24 provide an individual with a means to withdraw
25 affirmative express consent previously provided

1 by the individual to the covered entity with re-
2 spect to the transfer of the sensitive covered
3 data of the individual.

4 (B) REQUIREMENTS.—The means to with-
5 draw affirmative express consent described in
6 subparagraph (A) shall be—

7 (i) provided in a clear and con-
8 spicuous manner; and

9 (ii) as easy for a reasonable individual
10 to use as the means by which the indi-
11 vidual provided affirmative express con-
12 sent.

13 (c) ADDITIONAL PROTECTIONS FOR BIOMETRIC IN-
14 FORMATION AND GENETIC INFORMATION.—

15 (1) IN GENERAL.—A covered entity, or a serv-
16 ice provider on behalf of a covered entity, may not
17 collect, process, or retain biometric information or
18 genetic information without the affirmative express
19 consent of the individual to whom such data per-
20 tains, unless for a purpose expressly permitted by
21 paragraph (1), (2), (3), (4), (9), (10), (11), (12), or
22 (13) of subsection (d) and if such collection, proc-
23 essing, or retention is essential for such purpose.

24 (2) RETENTION.—A covered entity, or service
25 provider acting on behalf of a covered entity, shall

1 not retain biometric or genetic information beyond
2 the point for which a purpose that an individual pro-
3 vided affirmative express consent under (c)(1) has
4 been satisfied or within 3 years of the individual's
5 last interaction with the covered entity or service
6 provider, whichever occurs first, unless such reten-
7 tion is essential for a purpose expressly permitted
8 under paragraphs (1) through (4) or paragraphs (9)
9 through (13) of subsection (d).

10 (3) TRANSFER.—A covered entity, or a service
11 provider on behalf of a covered entity, may not
12 transfer biometric information or genetic informa-
13 tion to a third party without the affirmative express
14 consent of the individual to whom such data pertains
15 unless for a purpose expressly permitted by para-
16 graph (2), (3), (4), (8), (9), (11), or (12) of sub-
17 section (d).

18 (4) WITHDRAWAL OF AFFIRMATIVE EXPRESS
19 CONSENT.—

20 (A) IN GENERAL.—A covered entity shall
21 provide an individual with a means to withdraw
22 affirmative express consent previously provided
23 by the individual to the covered entity with re-
24 spect to the biometric information or genetic in-
25 formation of the individual.

1 (B) REQUIREMENTS.—The means to with-
2 draw affirmative express consent described in
3 subparagraph (A) shall be—

4 (i) provided in a clear and con-
5 spicuous manner; and

6 (ii) as easy for a reasonable individual
7 to use as the means by which the indi-
8 vidual provided affirmative express con-
9 sent.

10 (d) PERMITTED PURPOSES.—A covered entity, or
11 service provider on behalf of a covered entity, may collect,
12 process, retain, or transfer covered data for the following
13 purposes, if the covered entity or service provider can dem-
14 onstrate that the collection, processing, retention, or
15 transfer is necessary, proportionate, and limited to such
16 purpose:

17 (1) To protect data security as described in sec-
18 tion 9, protect against spam, and maintain networks
19 and systems, including through diagnostics, debug-
20 ging, and repairs.

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

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

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

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

10 (6) To conduct market research.

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

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

17 (B) conduct internal research or analytics
18 to improve a product or service of the covered
19 entity; or

20 (C) conduct a public or peer-reviewed sci-
21 entific, historical, or statistical research project
22 that—

23 (i) is in the public interest; and

24 (ii) adheres to all relevant laws and
25 regulations governing such research, in-

1 cluding regulations for the protection of
2 human subjects.

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

10 (A) a notice describing such transfer, in-
11 cluding the name of the entity or entities receiv-
12 ing the covered data of the individual and the
13 privacy policies of such entity or entities as de-
14 scribed in section 4; and

15 (B) a reasonable opportunity to—

16 (i) withdraw any previously given con-
17 sent in accordance with the requirements
18 of affirmative express consent under this
19 Act related to the covered data of the indi-
20 vidual; and

21 (ii) to request the deletion of the cov-
22 ered data of the individual, as described in
23 section 5.

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

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

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

12 (11) To prevent, detect, protect against, or re-
13 spond to an ongoing or imminent security incident.
14 For the purposes of this paragraph, security is de-
15 fined as relating to network security or physical se-
16 curity, including an intrusion or trespass, medical
17 alerts, fire alarms, and access control.

18 (12) To prevent, detect, protect against, or re-
19 spond to an imminent or ongoing public safety inci-
20 dent (such as mass casualty events, natural disas-
21 ters, or national security incidents). This paragraph
22 does not permit the transfer of covered data for pay-
23 ment or other valuable consideration to a govern-
24 ment entity.

1 (13) Except for health information, to prevent,
2 detect, protect against, investigate, or respond to
3 criminal activity. This paragraph does not permit
4 the transfer of covered data for payment or other
5 valuable consideration to a government entity.

6 (14) Except for sensitive covered data and only
7 with respect to covered data previously collected in
8 accordance with this Act, to process such data as
9 necessary to provide first party or contextual adver-
10 tising by the covered entity for individuals.

11 (15) Except for sensitive covered data and only
12 with respect to covered data previously collected in
13 accordance with this Act, for an individual who has
14 not opted out of targeted advertising pursuant to
15 section 6, processing or transferring covered data to
16 provide targeted advertising.

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

20 (f) JOURNALISM.—Nothing in this Act may be con-
21 strued to limit or diminish freedoms guaranteed under the
22 First Amendment to the Constitution.

23 **SEC. 4. TRANSPARENCY.**

24 (a) IN GENERAL.—Each covered entity and service
25 provider shall make publicly available, in a clear, con-

1 spicuous, not misleading, easy-to-read, and readily acces-
2 sible manner, a privacy policy that provides a detailed and
3 accurate representation of the data collection, processing,
4 retention, and transfer activities of the entity.

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

8 (1) The identity and the contact information
9 of—

10 (A) the covered entity or service provider
11 to which the privacy policy applies including a
12 point of contact and a monitored email address,
13 as applicable specific to data privacy and data
14 security inquiries; and

15 (B) any affiliate within the same corporate
16 structure as the covered entity or service pro-
17 vider, to which the covered entity or service pro-
18 vider may transfer data that—

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

21 or

22 (ii) has different contact information
23 than the covered entity or service provider.

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

1 (A) The categories of covered data the cov-
2 ered entity or service provider collects, proc-
3 esses, or retains; and

4 (B) The processing purposes for each such
5 category of covered data

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

8 (A) each category of service provider and
9 third party to which the covered entity or serv-
10 ice provider transfers covered data;

11 (B) the name of each data broker to which
12 the covered entity or service provider transfers
13 covered data; and

14 (C) the purposes for which such data is
15 transferred.

16 (4) The length of time the covered entity or
17 service provider intends to retain each category of
18 covered data, including sensitive covered data, or, if
19 it is not possible to identify the length of time, the
20 criteria used to determine the length of time the cov-
21 ered entity or service provider intends to retain each
22 category of covered data.

23 (5) A prominent description of how an indi-
24 vidual can exercise the rights of the individual under
25 sections 5 and 6.

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

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

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

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

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

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

18 (d) ACCESSIBILITY.—The covered entity or service
19 provider shall provide the disclosures under this section
20 in a manner that is reasonably accessible to and usable
21 by individuals living with disabilities.

22 (e) MATERIAL CHANGES.—

23 (1) NOTICE AND OPT OUT.—A covered entity
24 that makes a material change to its privacy policy

1 or practices with respect to previously collected cov-
2 ered data shall—

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

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

7 (ii) a means to opt out of the proc-
8 essing or transfer of such previously col-
9 lected covered data pursuant to such mate-
10 rial change; and

11 (B) with respect to the covered data of any
12 individual who opts out using the means de-
13 scribed in subparagraph (A)(ii), discontinue the
14 processing or transfer of such previously col-
15 lected covered data, unless such processing or
16 transfer is strictly necessary to provide a prod-
17 uct or service specifically requested by the indi-
18 vidual.

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

1 technology and the nature of the relationship be-
2 tween the entity and the individual.

3 (3) CLARIFICATION.—Except as provided in
4 paragraph (1)(B), nothing in this subsection may be
5 construed to affect the requirements for covered en-
6 tities section 3, 5, or 6.

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

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

11 (A) IN GENERAL.—Beginning after the
12 date of enactment of this Act, each large data
13 holder shall—

14 (i) retain and publish on the website
15 of the large data holder a copy of each pre-
16 vious version of its privacy policy (as de-
17 scribed in subsection (d)) for not less than
18 10 years; and

19 (ii) make publicly available on its
20 website, in a clear, conspicuous, and read-
21 ily accessible manner, a log that describes
22 the date and nature of each material
23 change to its privacy policy of the large
24 data holder during the preceding 10-year
25 period in a manner that is sufficient for a

1 reasonable individual to understand the ef-
2 fect of each material change.

3 (B) EXCLUSION.—The obligations in this
4 paragraph do not apply to material changes to
5 previous versions of a large data holder’s pri-
6 vacy policy that precede the date of the enact-
7 ment of this Act.

8 (2) SHORT FORM NOTICE TO CONSUMERS.—

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

14 (i) is concise, clear, conspicuous, and
15 not misleading;

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

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

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

4 (iv) is not more than 500 words in
5 length.

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

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

14 (a) ACCESS TO, AND CORRECTION, DELETION, AND
15 PORTABILITY OF, COVERED DATA.—After receiving a
16 verified request from an individual, a covered entity shall
17 provide the individual with the right to—

18 (1) access—

19 (A) in a format that can be naturally read
20 by a human, the covered data of the individual
21 (or an accurate representation of the covered
22 data of the individual if the covered data is no
23 longer in the possession of the covered entity or
24 a service provider acting on behalf of the cov-
25 ered entity) that is collected, processed, or re-

1 tained by the covered entity or any service pro-
2 vider of the covered entity;

3 (B) the name of any third party or service
4 provider to whom the covered entity has trans-
5 ferred the covered data of the individual, as well
6 as the categories of sources from which the cov-
7 ered data was collected; and

8 (C) a description of the purpose for which
9 the covered entity transferred the covered data
10 of the individual to a third party or service pro-
11 vider;

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

19 (3) delete covered data of the individual that is
20 collected, processed, or retained by the covered enti-
21 ty and, for covered data that has been transferred,
22 request that the covered entity notify any third
23 party or service provider to which the covered entity
24 transferred such covered data of the deletion request
25 of the individual; and

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

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

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

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

13 (1) shall provide an individual with the oppor-
14 tunity to exercise each of the rights described in
15 subsection (a); and

16 (2) with respect to—

17 (A) the first 3 instances that an individual
18 exercises any right described in subsection (a)
19 during any 12-month period, shall allow the in-
20 dividual to exercise such right free of charge;
21 and

22 (B) any time beyond the initial 3 times de-
23 scribed in subparagraph (A), may charge a rea-
24 sonable fee for each additional request to exer-

1 eise any such right during such 12-month pe-
2 riod.

3 (c) TIMING.—

4 (1) IN GENERAL.—Subject to subsections (b),
5 (d), and (e), each request under subsection (a) shall
6 be completed by any—

7 (A) any large data holder or data broker
8 not later than 15 calendar days of such request
9 from an individual, unless it is impossible or de-
10 monstrably impracticable to verify the relevant
11 individual; or

12 (B) with respect to a covered entity that is
13 not a large data holder, not later than 30 cal-
14 endar days of such request from an individual,
15 unless it is impossible or demonstrably imprac-
16 ticable to verify the relevant individual.

17 (2) EXTENSION.—The response period required
18 under paragraph (1) may be extended once by not
19 more than the applicable time period described in
20 such paragraph when reasonably necessary, consid-
21 ering the complexity and number of the individual’s
22 requests, provided that the covered entity informs
23 the individual of any such extension within the ini-
24 tial response period, together with the reason for the
25 extension.

1 (d) VERIFICATION.—

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

5 (A) the individual whose covered data is
6 the subject of the request ; or

7 (B) or an individual authorized to make
8 such a request on behalf of the individual whose
9 covered data is the subject of the request.

10 (2) ADDITIONAL INFORMATION.—If a covered
11 entity cannot make the verification described in
12 paragraph (1), the covered entity—

13 (A) may request that the individual mak-
14 ing such request provide any additional infor-
15 mation necessary for the sole purpose of
16 verifying the identity of the individual; and

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

20 (e) EXCEPTIONS.—

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

1 (A) cannot reasonably verify that the indi-
2 vidual making such request is the individual
3 whose covered data is the subject of the request
4 or an individual authorized to make such a re-
5 quest on behalf of the individual whose covered
6 data is the subject of the request;

7 (B) determines that exercise of the right
8 would require access to the sensitive covered
9 data of an individual other than the individual
10 whose covered data is the subject of the re-
11 quest;

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

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

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

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

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

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

8 (2) PERMISSIVE EXCEPTIONS.—

9 (A) IN GENERAL.—A covered entity may
10 decline, with adequate explanation to the indi-
11 vidual making the request, to comply with a re-
12 quest to exercise a right described in subsection
13 (a), in whole or in part, that would—

14 (i) be demonstrably impossible due to
15 technology or cost, and the covered entity
16 shall provide a detailed description to the
17 requestor regarding the inability to comply
18 with the request due to technology or cost;

19 (ii) delete covered data reasonably
20 necessary to perform a contract between
21 the covered entity and the individual;

22 (iii) with respect to a right described
23 under paragraph (1) or (4) of subsection
24 (a), require the covered entity to release

1 trade secrets or other privileged, propri-
2 etary, or confidential business information;

3 (iv) prevent a covered entity from
4 being able to maintain a confidential
5 record of opt out requests pursuant to sec-
6 tion 6 that is maintained solely for the
7 purpose of preventing covered data of an
8 individual from being continuing to be col-
9 lected after the individual submitted an opt
10 out request; or

11 (v) with regard to deletion requests,
12 require a private elementary or secondary
13 school as defined by State law and private
14 institutions of higher education as defined
15 by title I of the Higher Education Act of
16 1965, to delete covered data that would
17 unreasonably interfere with the provision
18 of education services by or the ordinary op-
19 eration of the school or institution.

20 (3) RULE OF CONSTRUCTION.—This section
21 may not be construed to require a covered entity
22 to—

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

1 entity for any purpose other than completing
2 such transaction;

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

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

8 (4) PARTIAL COMPLIANCE.—In the event a cov-
9 ered entity makes a permissive exception under
10 paragraph (2), the covered entity shall partially com-
11 ply with the remainder of the applicable request if
12 partial compliance is possible and not unduly bur-
13 densome.

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

19 (6) ADDITIONAL EXCEPTIONS.—

20 (A) IN GENERAL.—The Commission may
21 promulgate regulations, in accordance with sec-
22 tion 553 of title 5, United States Code, to es-
23 tablish additional permissive exceptions nec-
24 essary to protect the rights of individuals, to al-
25 leviate undue burdens on covered entities, to

1 prevent unjust or unreasonable outcomes from
2 the exercise of access, correction, deletion, or
3 portability rights, or as otherwise necessary to
4 fulfill the purposes of this section.

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

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

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

20 (A) the covered data is exclusively on-de-
21 vice data; and

22 (B) the individual can exercise any such
23 right using clear and conspicuous on-device con-
24 trols.

1 (f) LARGE DATA HOLDER METRICS REPORTING.—

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

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

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

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

11 (C) The number of verified requests to opt-
12 out of covered data transfers under section
13 6(a)(1).

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

17 (E) For each category of request described
18 in subparagraph (A), (B), (C), or (D), the num-
19 ber of such requests that the large data holder
20 complied with in whole or in part.

21 (F) For each category of request described
22 in subparagraph (A), (B), (C), or (D), the aver-
23 age number of days within which such large
24 data holder substantively responded to the re-
25 quest.

1 (2) PUBLIC DISCLOSURE.—Disclose, not later
2 than July 1 of each calendar year, the information
3 compiled under paragraph (1)—

4 (A) in the privacy policy of the large data
5 holder; or

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

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

15 (h) ACCESSIBILITY.—

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

21 (2) INDIVIDUALS LIVING WITH DISABILITIES.—
22 The mechanisms by which a covered entity enables
23 individuals to make a request to exercise a right de-
24 scribed in subsection (a) shall be readily accessible
25 and usable by individuals living with 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 an individual the following opt-out rights with respect to
5 the covered data of the individual:

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

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

11 (B) allow an individual to make an opt-out
12 designation pursuant to subparagraph (A)
13 through an opt-out mechanism as described in
14 subsection (b); and

15 (C) abide by an opt-out designation made
16 pursuant to subparagraph (A) and commu-
17 nicate such designation to all relevant service
18 providers.

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

22 (A) provide an individual with a clear and
23 conspicuous means to opt out of the processing
24 of covered data of the individual in furtherance
25 of targeted advertising;

1 (B) allow an individual to make an opt-out
2 designation with respect to targeted advertising
3 through an opt-out mechanism as described in
4 subsection (b); and

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

8 (b) CENTRALIZED CONSENT AND OPT-OUT MECHA-
9 NISM.—

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

22 (A) ensures that the opt-out preference
23 signal—

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

1 (ii) does not require that the indi-
2 vidual provide additional information be-
3 yond what is reasonably necessary to indi-
4 cate such preference;

5 (iii) clearly represents the preference
6 of an individual and is free of defaults con-
7 straining or presupposing such preference;

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

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

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

17 (B) provides a mechanism for the indi-
18 vidual to selectively opt out of the collection,
19 processing, retention, or transfer of covered
20 data by a covered entity, without affecting the
21 preferences of the individual with respect to
22 other entities or disabling the opt-out pref-
23 erence signal globally;

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

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

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

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

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

12 (a) DARK PATTERNS PROHIBITED.—

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

15 (A) divert the attention of an individual
16 from any notice required under this Act;

17 (B) impair the ability of an individual to
18 exercise any right under this Act; or

19 (C) obtain, infer, or facilitate the consent
20 of an individual for any action that requires the
21 consent of an individual under this Act.

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

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 goods or services, charging different
14 prices or rates for goods or services, or providing a dif-
15 ferent level of quality of goods 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, quality
22 or selection of goods or services to an indi-
23 vidual, including offering goods or services
24 for no fee, if the offering is in connection
25 with the voluntary participation of an indi-

1 individual in a bona fide loyalty program, pro-
2 vided 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 an individual in
11 the manner set forth in section
12 3(b)(2);

13 (III) the covered entity abides by
14 the exercise by the individual of any
15 right provided by section 3(b)(2), 5,
16 or 6; and

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

22 (ii) different prices or functionalities
23 with respect to a product or service based
24 on the decision of an individual to termi-
25 nate membership in a bona fide loyalty

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

5 (B) BONA FIDE LOYALTY PROGRAM DE-
6 FINED.—For purposes of this section, the term
7 “bona fide loyalty program” includes rewards,
8 premium features, discounts, or club card pro-
9 grams offered by a covered entity that is not a
10 high-impact social media company or data
11 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 provision 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.—Each covered entity or serv-
6 ice provider shall establish, implement, and maintain
7 reasonable data security practices to protect—

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

10 (B) covered data of the entity against un-
11 authorized access.

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

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

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

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

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

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

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

19 (2) PREVENTIVE AND CORRECTIVE ACTION.—

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

1 role of the entity in collecting, processing, re-
2 taining, or transferring the data, which may in-
3 clude implementing administrative, technical, or
4 physical safeguards or changes to data security
5 practices or the architecture, installation, or im-
6 plementation of network or operating software.

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

14 (3) INFORMATION RETENTION AND DIS-
15 POSAL.—Disposing of covered data (either by or at
16 the direction of the covered entity) that is required
17 to be deleted by law or is no longer necessary for the
18 purpose for which the data was collected, processed,
19 retained, or transferred, unless an individual has
20 provided affirmative express consent for retention.
21 Such disposal shall include destroying, permanently
22 erasing, or otherwise modifying the covered data to
23 make such data permanently unreadable or indeci-
24 pherable and unrecoverable to ensure ongoing com-
25 pliance with this section.

1 (4) RETENTION SCHEDULE.—Developing, main-
2 taining, and adhering to a retention schedule for
3 covered data consistent with the practices and proce-
4 dures required in paragraph (3).

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

8 (6) INCIDENT RESPONSE.—Implementing pro-
9 cedures to detect, respond to, and recover from data
10 security incidents, including breaches.

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

16 **SEC. 10. EXECUTIVE RESPONSIBILITY.**

17 (a) DESIGNATION OF PRIVACY AND DATA SECURITY
18 OFFICERS.—

19 (1) DESIGNATION.—

20 (A) IN GENERAL.—Except for an entity
21 that is a large data holder a covered entity or
22 service provider shall designate 1 or more quali-
23 fied employees to serve as a privacy or data se-
24 curity officers.

1 (B) REQUIREMENTS FOR OFFICERS.—An
2 employee who is designated by a covered entity
3 or service provider as a privacy or data security
4 officer shall, at a minimum—

5 (i) implement a data privacy program
6 and a data security program to safeguard
7 the privacy and security of covered data in
8 compliance with the requirements of this
9 Act; and

10 (ii) facilitate the ongoing compliance
11 of the covered entity or service provider
12 with this Act.

13 (2) REQUIREMENTS FOR LARGE DATA HOLD-
14 ERS.—

15 (A) DESIGNATION.—A covered entity or
16 service provider that is a large data holder shall
17 designate 1 qualified employee to serve as a pri-
18 vacy officer and 1 qualified employee to serve
19 as a data security officer.

20 (B) ANNUAL CERTIFICATION.—

21 (i) IN GENERAL.—Beginning on the
22 date that is 1 year after the date of the en-
23 actment of this Act, the chief executive of-
24 ficer of a large data holder (or, if the large
25 data holder does not have a chief executive

1 officer, the highest ranking officer of the
2 large data holder), and each privacy officer
3 and data security officer of such large data
4 holder designated under subparagraph (A),
5 shall annually certify to the Commission,
6 in a manner specified by the Commission,
7 that the large data holder maintains—

8 (I) internal controls reasonably
9 designed to comply with this Act; and

10 (II) internal reporting structures
11 (as described in subparagraph (C)) to
12 ensure that such certifying officers
13 are involved in, and responsible for,
14 decisions that impact compliance by
15 the large data holder with this Act.

16 (ii) REQUIREMENTS.—A certification
17 submitted under clause (i) shall be based
18 on a review of the effectiveness of the in-
19 ternal controls and reporting structures of
20 the large data holder that is conducted by
21 the certifying officers not more than 90
22 days before the submission of the certifi-
23 cation.

24 (C) INTERNAL REPORTING STRUCTURE RE-
25 QUIREMENTS.—At least 1 of the officers de-

1 scribed in subparagraph (A) shall, either di-
2 rectly or through a supervised designee—

3 (i) establish processes to periodically
4 review and update, as necessary, the pri-
5 vacy and security policies, practices, and
6 procedures of the large data holder;

7 (ii) conduct biennial and comprehen-
8 sive audits to ensure the policies, practices,
9 and procedures of the large data holder
10 comply with this Act and, upon request,
11 make such audits available to the Commis-
12 sion;

13 (iii) develop a program to educate and
14 train employees about the requirements of
15 this Act;

16 (iv) maintain updated, accurate, clear,
17 and understandable records of all signifi-
18 cant privacy and data security practices of
19 the large data holder; and

20 (v) serve as the point of contact be-
21 tween the large data holder and enforce-
22 ment authorities.

23 (D) PRIVACY IMPACT ASSESSMENTS.—

24 (i) IN GENERAL.—Not later than 1
25 year after the date of the enactment of this

1 Act or 1 year after the date on which an
2 entity first meets the definition of a large
3 data holder, whichever is earlier, and bien-
4 nially thereafter, each large data holder
5 shall conduct a privacy impact assessment
6 that weighs the benefits of the covered
7 data collection, processing, retention, and
8 transfer practices of the entity against the
9 potential adverse consequences of such
10 practices to individual privacy.

11 (ii) ASSESSMENT REQUIREMENTS.—A
12 privacy impact assessment required under
13 clause (i) shall be—

14 (I) reasonable and appropriate in
15 scope given—

16 (aa) the nature and volume
17 of the covered data collected,
18 processed, retained, or trans-
19 ferred by the large data holder;
20 and

21 (bb) the potential risks
22 posed to the privacy of individ-
23 uals by the collection, processing,
24 retention, and transfer of covered
25 data by the large data holder;

1 (II) documented in written form
2 and maintained by the large data
3 holder unless rendered out of date by
4 a subsequent assessment conducted
5 under clause (i); and

6 (III) approved by the privacy of-
7 ficer of the large data holder.

8 (iii) ADDITIONAL FACTORS TO IN-
9 CLUDE IN ASSESSMENT.—In assessing pri-
10 vacy risks for purposes of an assessment
11 conducted under subparagraph (A, includ-
12 ing substantial privacy risks, the large
13 data holder shall include reviews of the
14 means by which technologies, including
15 blockchain and distributed ledger tech-
16 nologies, and other emerging technologies,
17 including privacy enhancing technologies,
18 are used to secure covered data.

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

20 (a) SERVICE PROVIDERS.—

21 (1) IN GENERAL.—A service provider—

22 (A) shall adhere to the instructions of a
23 covered entity and only collect, process, retain,
24 or transfer service provider data to the extent
25 necessary, proportionate, and limited to provide

1 a service requested by the covered entity, as set
2 out in the contract required under paragraph
3 (2);

4 (B) may not collect, process, retain, or
5 transfer covered data if the service provider has
6 actual knowledge that a covered entity violated
7 this Act with respect to such data;

8 (C) shall assist a covered entity in fulfilling
9 the covered entity's obligations to respond to
10 consumer rights requests pursuant to sections
11 5, 6, and 14 by appropriate technical and orga-
12 nizational measures, taking into account the na-
13 ture of the processing and the information rea-
14 sonably available to the service provider;

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

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

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

11 (G) shall develop, implement, and maintain
12 reasonable administrative, technical, and phys-
13 ical safeguards that are designed to protect the
14 security and confidentiality of covered data the
15 service provider processes consistent with sec-
16 tion 9; and

17 (H) shall—

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

20 (ii) arrange for a qualified and inde-
21 pendent assessor to conduct an assessment
22 of the service provider's policies and tech-
23 nical and organizational measures in sup-
24 port of the obligations under this Act,
25 using an appropriate and accepted control

1 standard or framework and assessment
2 procedure for such assessments and report
3 the results of such assessment to the cov-
4 ered entity.

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

7 (A) shall govern the service provider’s data
8 processing procedures with respect to any col-
9 lection, processing, retention, or transfer per-
10 formed on behalf of the covered entity;

11 (B) shall clearly set forth—

12 (i) instructions for collecting, proc-
13 essing, retaining, or transferring data;

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

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

18 (iv) the duration of the processing or
19 retention; and

20 (v) the rights and obligations of both
21 parties;

22 (C) shall not relieve a covered entity or
23 service provider of any obligation under this
24 Act; and

25 (D) shall prohibit—

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

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

15 (b) THIRD PARTIES.—A third party—

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

18 (A) in the case of sensitive covered data,
19 the purpose for which an individual gave af-
20 firmative express consent for the transfer of the
21 individual's sensitive covered data; or

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

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

10 (3) shall be exempt from the requirements of
11 section 3(b) with respect to third-party data, but
12 shall otherwise have the same responsibilities and
13 obligations as a covered entity with respect to such
14 data under all other provisions of this Act.

15 (c) RULES OF CONSTRUCTION.—

16 (1) SUCCESSIVE ACTOR VIOLATIONS.—

17 (A) IN GENERAL.—With respect to a viola-
18 tion of this Act by a service provider or third
19 party regarding covered data received by the
20 service provider or third party from a covered
21 entity, the covered entity that transferred such
22 covered data to the service provider or third
23 party shall not be in violation of this Act if the
24 covered entity transferred the covered data to
25 the service provider or third party in compli-

1 ance with the requirements of this Act and, at
2 the time of transferring such covered data, the
3 entity did not have actual knowledge, or reason
4 to believe, that the service provider or third
5 party intended to violate this Act.

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

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

21 (d) DUE DILIGENCE.—

22 (1) SERVICE PROVIDER SELECTION.—A covered
23 entity shall exercise reasonable due diligence in se-
24 lecting a service provider.

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

4 (3) GUIDANCE.—Not later than 2 years after
5 the date of enactment of this Act, the Commission
6 shall publish guidance regarding compliance with
7 this subsection.

8 **SEC. 12. DATA BROKERS.**

9 (a) NOTICE.—A data broker shall—

10 (1) establish and maintain a publicly accessible
11 website; and

12 (2) place a clear, conspicuous, not misleading,
13 and readily accessible notice on such publicly acces-
14 sible website, and any mobile application of the data
15 broker, that—

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

20 (B) an individual may exercise a right de-
21 scribed in section 5 and 6, and includes a link
22 or other tool to allow an individual to exercise
23 such right;

24 (C) includes a link to the website estab-
25 lished under subsection (e)(3); and

1 (D) is reasonably accessible to and usable
2 by individuals living with disabilities.

3 (b) PROHIBITED PRACTICES.—A data broker may
4 not—

5 (1) advertise or market the access to or trans-
6 fer of covered data for the purposes of—

7 (A) stalking or harassing another indi-
8 vidual; or

9 (B) engaging in fraud, identity theft, or
10 unfair or deceptive acts or practices; or

11 (2) misrepresent the business practices of the
12 data broker.

13 (c) DATA BROKER REGISTRATION.—

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

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

24 (A) Pay to the Commission a registration
25 fee of \$100.

1 (B) Provide the Commission with the fol-
2 lowing information:

3 (i) The legal name and primary phys-
4 ical, email, and internet addresses of the
5 data broker.

6 (ii) A description of the categories of
7 covered data the data broker collects, proc-
8 esses, retains, or transfers.

9 (iii) The contact information of the
10 data broker, including the name of a con-
11 tact person, a monitored telephone num-
12 ber, a monitored e-mail address, a website,
13 and a physical mailing address.

14 (iv) A link to a website through which
15 an individual may easily exercise the rights
16 described in subsection (a)(2)(B).

17 (3) DATA BROKER REGISTRY.—

18 (A) ESTABLISHMENT.—The Commission
19 shall establish and maintain on a publicly avail-
20 able website a searchable list of data brokers
21 that are registered with the Commission under
22 this subsection.

23 (B) REQUIREMENTS.—the registry estab-
24 lished under subparagraph (A) shall—

1 (i) allows members of the public to
2 search for and identify data brokers;

3 (ii) include the information required
4 under paragraph (2)(B) for each data
5 broker; and

6 (iii) includes a mechanism by which
7 an individual may submit a request to all
8 registered data brokers that are not con-
9 sumer reporting agencies (as defined in
10 section 603(f) of the Fair Credit Reporting
11 Act (15 U.S.C. 1681a(f))), and to the ex-
12 tent such data brokers are not acting as
13 consumer reporting agencies (as so de-
14 fined) or service providers, a “Do Not Col-
15 lect” directive that results in registered
16 data brokers no longer collecting covered
17 data related to such individual without the
18 affirmative express consent of such indi-
19 vidual.

20 (4) DO NOT COLLECT REQUESTS.—

21 (A) COMPLIANCE.—Subject to subpara-
22 graph (B), each data broker that receives a re-
23 quest from an individual using the mechanism
24 established under paragraph (3)(B)(iii) shall
25 comply with such request not later than 30

1 days after the date on which the request is re-
2 ceived by the data broker.

3 (B) EXCEPTION.—A data broker may de-
4 cline to fulfill a request from an individual
5 where—

6 (i) the data broker has actual knowl-
7 edge that the individual has been convicted
8 of a crime related to the abduction or sex-
9 ual exploitation of a child, and

10 (ii) the data collected by the data
11 broker is necessary

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

14 (II) for the congressionally des-
15 igned entity that serves as the non-
16 profit national resource center and
17 clearinghouse to provide assistance to
18 victims, families, child-serving profes-
19 sionals, and the general public on
20 missing and exploited children.

21 (d) PENALTIES.—

22 (1) IN GENERAL.—Subject to paragraph (2) a
23 data broker that fails to comply with the provisions
24 of this section shall be liable for civil penalties as set

1 forth in subsections (l) and (m) of section 5 of the
2 Federal Trade Commission Act (15 U.S.C. 45).

3 (2) EXCEPTION.—A data broker that—

4 (A) fails to register with the Commission
5 as required by subsection (c) shall be liable
6 for—

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

10 (ii) an amount equal to the registra-
11 tion fees due under subsection (c)(2)(A)
12 for each year that the data broker failed to
13 register as required under subsection
14 (c)(1); or

15 (B) fails to provide notice as required by
16 subsection (a) shall be liable for a civil penalty
17 of \$100 for each day the data broker fails to
18 provide such notice, not to exceed a total of
19 \$10,000 for any year.

20 (3) RULE OF CONSTRUCTION.—Except as pro-
21 vided in paragraph (2), nothing in this subsection
22 may be construed as altering, limiting, or affecting
23 any enforcement authorities or remedies under this
24 Act.

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

2 (a) CIVIL RIGHTS PROTECTIONS.—

3 (1) IN GENERAL.—A covered entity or service
4 provider may not collect, process, retain, or transfer
5 covered data in a manner that discriminates in or
6 otherwise makes unavailable the equal enjoyment of
7 goods or services on the basis of race, color, religion,
8 national origin, sex, or disability.

9 (2) EXCEPTIONS.—This subsection does not
10 apply to—

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

13 (i) self-testing by a covered entity or
14 service provider to prevent or mitigate un-
15 lawful discrimination; or

16 (ii) diversifying an applicant, partici-
17 pant, or customer pool;

18 (B) any private club or other establishment
19 not open to the public, as described in section
20 201(e) of the Civil Rights Act of 1964 (42
21 U.S.C. 2000a(e)); or

22 (C) advertising, marketing, or soliciting
23 economic opportunities or benefits to underrep-
24 resented populations or members of protected
25 classes as described in paragraph (1).

26 (b) FTC ENFORCEMENT ASSISTANCE.—

1 (1) IN GENERAL.—Whenever the Commission
2 obtains information that a covered entity or service
3 provider may have collected, processed, retained, or
4 transferred covered data in violation of subsection
5 (a), the Commission shall transmit such information,
6 as allowable under Federal law, to any Executive
7 agency with authority to initiate enforcement actions
8 or proceedings relating to such violation.

9 (2) ANNUAL REPORT.—Not later than 3 years
10 after the date of the enactment of this Act, and an-
11 nually thereafter, the Commission shall submit to
12 Congress a report that includes a summary of—

13 (A) the types of information the Commis-
14 sion transmitted to Executive agencies under
15 paragraph (1) during the previous 1-year pe-
16 riod; and

17 (B) how such information relates to Fed-
18 eral civil rights laws.

19 (3) TECHNICAL ASSISTANCE.—In transmitting
20 information to an Executive agency under paragraph
21 (1), the Commission may consult and coordinate
22 with, and provide technical and investigative assist-
23 ance, as appropriate, to such Executive agency.

24 (4) COOPERATION WITH OTHER AGENCIES.—
25 The Commission may implement this subsection by

1 executing agreements or memoranda of under-
2 standing with appropriate Executive agencies.

3 (c) COVERED ALGORITHM IMPACT AND EVALUA-
4 TION.—

5 (1) COVERED ALGORITHM IMPACT ASSESS-
6 MENT.—

7 (A) IMPACT ASSESSMENT.—Notwith-
8 standing any other provision of law, not later
9 than 2 years after the date of the enactment of
10 this Act, and annually thereafter, a large data
11 holder that uses a covered algorithm in a man-
12 ner that poses a consequential risk of harm to
13 an individual or group of individuals and uses
14 such covered algorithm, solely or in part, to col-
15 lect, process, or transfer covered data shall con-
16 duct an impact assessment of such algorithm in
17 accordance with subparagraph (B).

18 (B) IMPACT ASSESSMENT SCOPE.—An im-
19 pact assessment required under subparagraph
20 (A) shall include the following:

21 (i) A detailed description of the design
22 process and methodologies of the covered
23 algorithm.

24 (ii) A statement of the purpose and
25 proposed uses of the covered algorithm.

1 (iii) A detailed description of the data
2 used by the covered algorithm, including
3 the specific categories of data that will be
4 processed as input and any data used to
5 train the model on which the covered algo-
6 rithm relies, if applicable.

7 (iv) A description of the outputs pro-
8 duced by the covered algorithm.

9 (v) An assessment of the necessity
10 and proportionality of the covered algo-
11 rithm in relation to its stated purpose.

12 (vi) A detailed description of steps the
13 large data holder has taken or will take to
14 mitigate potential harms from the covered
15 algorithm to an individual or group of indi-
16 viduals, including related to—

17 (I) covered minors;

18 (II) making or facilitating adver-
19 tising for, determining access to, or
20 restrictions on the use of housing,
21 education, employment, healthcare, in-
22 surance, or credit opportunities;

23 (III) determining access to, or re-
24 stricting the use of, any place of pub-
25 lic accommodation, particularly as

1 such harms relate to the protected
2 characteristics of individuals, includ-
3 ing race, color, religion, national ori-
4 gin, sex, or disability;

5 (IV) disparate impact on the
6 basis of race, color, religion, national
7 origin, sex, or disability status; or

8 (V) disparate impact on the basis
9 of political party registration status.

10 (2) ALGORITHM DESIGN EVALUATION.—Not-
11 withstanding any other provision of law, not later
12 than 2 years after the date of the enactment of this
13 Act, a covered entity or service provider that know-
14 ingly develops a covered algorithm that is designed,
15 solely or in part, to collect, process, or transfer cov-
16 ered data in furtherance of a consequential decision
17 shall, prior to deploying the covered algorithm in
18 interstate commerce, evaluate the design, structure,
19 and inputs of the covered algorithm, including any
20 training data used to develop the covered algorithm,
21 to reduce the risk of the potential harms identified
22 under paragraph (1)(B)(vi).

23 (3) OTHER CONSIDERATIONS.—

24 (A) FOCUS.—In complying with para-
25 graphs (1) and (2), a covered entity or service

1 provider may focus the impact assessment or
2 evaluation on any covered algorithm, or por-
3 tions of a covered algorithm, that will be put to
4 use and may reasonably contribute to the risk
5 of the potential harms identified under para-
6 graph (1)(B)(vi).

7 (B) AVAILABILITY.—

8 (i) IN GENERAL.—A covered entity or
9 service provider—

10 (I) shall, not later than 30 days
11 after completing an impact assess-
12 ment or evaluation under paragraph
13 (1) or (2), submit the impact assess-
14 ment or evaluation to the Commis-
15 sion;

16 (II) shall, upon request, make
17 such impact assessment or evaluation
18 available to Congress; and

19 (III) may make a summary of
20 such impact assessment or evaluation
21 publicly available in a place that is
22 easily accessible to individuals.

23 (ii) TRADE SECRETS.—A covered enti-
24 ty, or service provider may redact and seg-
25 regate any trade secret (as defined in sec-

1 tion 1839 of title 18, United States Code)
2 or other confidential or proprietary infor-
3 mation from public disclosure under this
4 subparagraph, and the Commission shall
5 abide by obligations under section 6(f) of
6 the Federal Trade Commission Act (15
7 U.S.C. 46(f)) in regard to such informa-
8 tion.

9 (C) LIMITATION ON ENFORCEMENT.—

10 (i) IN GENERAL.—The Commission
11 may not use any information obtained sole-
12 ly and exclusively through a disclosure of
13 information to the Commission in compli-
14 ance with this section for any purpose
15 other than enforcing this Act with the ex-
16 ception of enforcing consent orders, includ-
17 ing the study and report requirements in
18 paragraph (6).

19 (ii) PROVISION TO CONGRESS.—The
20 limitation described in clause (i) does not
21 preclude the Commission from providing
22 such information to Congress in response
23 to a subpoena.

24 (4) GUIDANCE.—Not later than 2 years after
25 the date of the enactment of this Act, the Commis-

1 sion shall, in consultation with the Secretary of
2 Commerce, publish guidance regarding compliance
3 with this section.

4 (5) RULEMAKING AND EXEMPTION.—The Com-
5 mission may promulgate regulations, in accordance
6 with section 553 of title 5, United States Code, as
7 necessary to establish processes by which a—

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

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

17 (6) STUDY AND REPORTS.—

18 (A) STUDY.—The Commission, in con-
19 sultation with the Secretary of Commerce, shall
20 conduct a study, to review impact assessments
21 and evaluations submitted under this sub-
22 section. Such study shall include an examina-
23 tion of—

24 (i) best practices for the assessment
25 and evaluation of covered algorithms; and

1 (ii) methods to reduce the risk of
2 harm to individuals that may be related to
3 the use of covered algorithms.

4 (B) REPORTS.—

5 (i) INITIAL REPORT.—Not later than
6 3 years after the date of the enactment of
7 this Act, the Commission, in consultation
8 with the Secretary of Commerce, shall sub-
9 mit to Congress a report containing the re-
10 sults of the study conducted under sub-
11 paragraph (A), together with recommenda-
12 tions for such legislation and administra-
13 tive action as the Commission determines
14 appropriate.

15 (ii) ADDITIONAL REPORTS.—Not later
16 than 3 years after submission of the initial
17 report required under clause (i), and as the
18 Commission determines necessary there-
19 after, the Commission shall submit to Con-
20 gress an updated version of such report.

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

22 (a) IN GENERAL.—An entity that uses a covered al-
23 gorithm to make or facilitate a consequential decision
24 shall—

25 (1) provide—

1 (A) notice to each individual subject to
2 such use of the covered algorithm; and

3 (B) an opportunity for the individual to
4 opt out of such use of covered algorithm; and

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

7 (b) NOTICE.—The notice required under subsection
8 (a)(1)(A) shall—

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

10 (2) provide meaningful information about how
11 the covered algorithm makes or facilitates a con-
12 sequential decision, including the range of potential
13 outcomes;

14 (3) be provided in each language in which such
15 entity—

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

18 (B) carries out activities related to such
19 product or service; and

20 (4) be reasonably accessible to and usable by in-
21 dividuals living with disabilities.

22 (d) GUIDANCE.—Not later than 2 years after the
23 date of the enactment of this Act, the Commission shall,
24 in consultation with the Secretary of Commerce, publish
25 guidance regarding compliance with this section.

1 (e) CONSEQUENTIAL DECISION DEFINED.—For the
2 purposes of this section, the term “consequential decision”
3 means a determination or an offer, including through ad-
4 vertisement, that uses covered data and relates to—

5 (1) the access of an individual or class of indi-
6 viduals to or equal enjoyment of housing, employ-
7 ment, education enrollment or opportunity,
8 healthcare, insurance, or credit opportunities; or

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

11 **SEC. 15. COMMISSION APPROVED COMPLIANCE GUIDE-**
12 **LINES.**

13 (a) APPLICATION FOR COMPLIANCE GUIDELINE AP-
14 PROVAL.—

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

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

1 (A) a description of how the proposed
2 guidelines will meet or exceed the requirements
3 of this Act;

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

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

10 (D) a description of an independent orga-
11 nization, not associated with any of the partici-
12 pating covered entities, that will administer the
13 proposed guidelines; and

14 (E) a description of how such entities will
15 be assessed for adherence to the proposed
16 guidelines by the independent organization de-
17 scribed in subparagraph (D).

18 (3) COMMISSION REVIEW.—

19 (A) INITIAL APPROVAL.—

20 (i) PUBLIC COMMENT PERIOD.—Not
21 later than 90 days after receipt of pro-
22 posed guidelines submitted pursuant to
23 paragraph (1), the Commission shall pub-
24 lish the application and provide an oppor-

1 tunity for public comment on such pro-
2 posed guidelines.

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

10 (I) meet or exceed requirements
11 of this Act;

12 (II) will provide for the regular
13 review and validation by an inde-
14 pendent organization to ensure that
15 the covered entity or entities continue
16 to meet or exceed the requirements of
17 this Act; and

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

1 eral for enforcement consistent with
2 section 18.

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

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

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

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

1 not later than 1 year after the date on
2 which the Commission received the submis-
3 sion for approval.

4 (b) WITHDRAWAL OF APPROVAL.—

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

16 (2) OPPORTUNITY TO CURE.—

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

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

1 (1) means any software or hardware solution,
2 cryptographic algorithm, or other technical process
3 of extracting the value of the information without
4 risking the privacy and security of the information;
5 and

6 (2) includes other technologies with
7 functionality similar to homomorphic encryption, dif-
8 ferential privacy, zero-knowledge proofs, synthetic
9 data generation, federated learning, and secure
10 multi-party computation.

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

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

19 (1) develop and implement a petition process
20 for covered entities to request to be a part of the
21 pilot program; and

22 (2) build an auditing system that leverages pri-
23 vacy-enhancing technologies to support the enforce-
24 ment actions of the Commission subject to the pilot
25 program.

1 (d) PETITION PROCESS.—A covered entity wishing to
2 be accepted into the pilot program established under sub-
3 section (b) shall demonstrate to the Commission that the
4 privacy-enhancing technologies to be used under the pilot
5 program by the covered entity will establish data security
6 practices that meet or exceed the requirements in section
7 9. If the covered entity demonstrates the privacy-enhanc-
8 ing technologies meet or exceed the requirements in sec-
9 tion 9, the Commission may accept the covered entity to
10 be a part of the pilot program.

11 (e) REQUIREMENTS.—In carrying out the pilot pro-
12 gram established under subsection (b), the Commission
13 shall—

14 (1) receive input from private, public, and aca-
15 demic stakeholders; and

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

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

1 (g) STUDY REQUIRED.—

2 (1) IN GENERAL.—Not later than 3 years after
3 the date of the enactment of this Act, the Comp-
4 troller General of the United States shall conduct a
5 study—

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

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

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

19 (2) INITIAL BRIEFING.—Not later than 1 year
20 after the date of the enactment of this Act, the
21 Comptroller General shall brief the Committee on
22 Energy and Commerce of the House of Representa-
23 tives and the Committee on Commerce, Science, and
24 Transportation of the Senate on the initial results of
25 the study conducted under paragraph (1).

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

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

17 (i) WITHDRAWAL FROM THE PILOT PROGRAM.—If at
18 any time the Commission determines that a covered entity
19 accepted to be a part of the pilot program established
20 under subsection (b) is no longer maintaining the use of
21 privacy-enhancing technologies, the Commission shall no-
22 tify the covered entity of the determination of the Commis-
23 sion to withdraw approval of such participation and the
24 basis for doing so. Not later than 180 days after the date
25 on which a covered entity receives such notice, the covered

1 entity may cure any alleged deficiency with the use of pri-
2 vacy-enhancing technologies and submit each proposed
3 cure to the Commission. If the Commission determines
4 that such cure eliminates the alleged deficiency, the Com-
5 mission may not withdraw approval of such participation.

6 (j) LIMITATIONS ON LIABILITY.—Any covered entity
7 that petitions, and is accepted, to be part of the pilot pro-
8 gram established under subsection (b), and actively imple-
9 ments and maintains the use of privacy-enhancing tech-
10 nologies, shall—

11 (1) for any action under section 17 or 18 for
12 a violation of section 9, be deemed to be in compli-
13 ance with section 9 with respect to covered data sub-
14 ject to the privacy-enhancing technologies; and

15 (2) for any action under section 19 for a viola-
16 tion of section 9, be entitled to a rebuttable pre-
17 sumption that such entity is in compliance with such
18 section with respect to the covered data subject to
19 the privacy-enhancing technologies.

20 **SEC. 17. ENFORCEMENT BY FEDERAL TRADE COMMISSION.**

21 (a) NEW BUREAU.—

22 (1) IN GENERAL.—The Commission shall estab-
23 lish, within the Commission, a new bureau com-
24 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 authority of the Com-
6 mission 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 the enactment of this Act.

10 (b) ENFORCEMENT BY COMMISSION.—

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

18 (2) POWERS OF COMMISSION.—

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

1 the Federal Trade Commission Act (15 U.S.C.
2 41 et seq.) were incorporated into and made a
3 part of this Act.

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

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

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

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

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

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

9 (B) DEPOSITS.—

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

17 (ii) DEPOSITS FROM ATTORNEY GEN-
18 ERAL.—The Attorney General shall deposit
19 into the Victims Relief Fund the amount
20 of any civil penalty obtained against any
21 entity in any judicial or administrative ac-
22 tion the Attorney General commences on
23 behalf of the Commission to enforce this
24 Act or a regulation promulgated under this
25 Act.

1 (C) USE OF FUND AMOUNTS.—

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

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

19 (I) consumer or business edu-
20 cation relating to privacy and secu-
21 rity; or

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

25 (D) CALCULATION.—Any amount—

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

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

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

25 (c) REPORT.—

1 (1) IN GENERAL.—Not later than 4 years after
2 the date of the enactment of this Act, and annually
3 thereafter, the Commission shall submit to Congress
4 a report—

5 (A) describing investigations with respect
6 to violations of this Act, including—

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

9 (ii) the number of such investigations
10 the Commission closed with no official
11 agency action;

12 (iii) the disposition of such investiga-
13 tions, if such investigations have concluded
14 and resulted in official agency action; and

15 (iv) for each investigation that was
16 closed with no official agency action, the
17 industry sectors of the covered entities
18 subject to each investigation; and

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

24 (3) ANNUAL PLAN.—Not later than 540 days
25 after the enactment of this Act, and annually there-

1 after, the Commission shall submit to Congress plan
2 for the next calendar year describing the projected
3 activities of the Commission under this Act, includ-
4 ing—

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

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

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

14 (D) any plans to restructure the Commis-
15 sion or establish, alter, or terminate working
16 groups; and

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

21 **SEC. 18. ENFORCEMENT BY STATES.**

22 (a) CIVIL ACTION.—

23 (1) IN GENERAL.—In any case in which the at-
24 torney general of a State, the chief consumer protec-
25 tion officer of a State, or an officer or office of a

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

13 (A) enjoin such act or practice;

14 (B) enforce compliance with this Act or the
15 regulations promulgated under this Act;

16 (C) obtain civil penalties;

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

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

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

24 (2) LIMITATION.—In any case with respect to
25 which the attorney general of a State, the chief con-

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

9 (b) RIGHTS OF THE COMMISSION.—

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

17 (A) be heard on all matters arising in such
18 action; and

19 (B) file petitions for appeal of a decision in
20 such action.

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

1 tify the Commission immediately after initiating the
2 civil action.

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

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

24 (e) VENUE; SERVICE OF PROCESS.—

1 (1) VENUE.—Any action brought under sub-
2 section (a) may be brought in Federal district court
3 of the United States that meets applicable require-
4 ments relating to venue under section 1391 of title
5 28, United States Code.

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

9 (A) is an inhabitant; or

10 (B) may be found.

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

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

20 (2) the contingency fees, hourly rates, and
21 other costs of hiring or contracting with outside
22 firms;

23 (3) the types of matters for which outside firms
24 are hired or contracted with for;

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

3 (5) the practices State attorneys general set in
4 place to protect sensitive information that would be-
5 come accessible by outside firms while they are as-
6 sisting in such enforcement efforts;

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

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

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

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

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

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

4 (h) CALCULATION.—Any amount that a court orders
5 an entity to pay to an individual under this section shall
6 be offset by any amount the person received from an ac-
7 tion brought against the entity for the same violation
8 under section 17 or 19.

9 **SEC. 19. ENFORCEMENT BY PERSONS.**

10 (a) ENFORCEMENT BY INDIVIDUALS.—

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

23 (2) RELIEF.—

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

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

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

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

8 (iii) declaratory relief; and

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

11 (B) BIOMETRIC AND GENETIC INFORMA-
12 TION.—In a civil action brought under para-
13 graph (1) for a violation of this Act with re-
14 spect to section 3(e), in which the plaintiff pre-
15 vails, if the conduct underlying the violation oc-
16 curred primarily and substantially in Illinois, in
17 which the plaintiff prevails the court may award
18 the plaintiff—

19 (i) for a violation involving biometric
20 information, the same relief as set forth in
21 section 20 of the Biometric Information
22 Privacy Act (740 ILCS 14/20), as such
23 statute read on January 1, 2024; or

24 (ii) for a violation involving genetic in-
25 formation, the same relief as set forth in

1 section 40 of the Genetic Information Pri-
2 vacy Act 740 ILCS 513/40), as such stat-
3 ute read on January 1, 2024.

4 (C) DATA SECURITY.—

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

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

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

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

8 (aa) A government identifier
9 as defined in section 2(34)(A)(i).

10 (bb) A financial account
11 number as defined in section
12 2(34)(A)(iv).

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

19 (dd) Biometric information.

20 (ee) Genetic information.

21 (D) LIMITATIONS ON DUAL ACTIONS.—

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

1 the entity for the same violation under section
2 17 or 18.

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

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

12 (2) EFFECT OF CURE.—In the event a cure is
13 possible, if within the 30 days the entity cures the
14 noticed violation and provides the person an express
15 written statement that the violation has been cured
16 and that no such further violations shall occur, an
17 action for injunctive relief may not be permitted.

18 (3) INJUNCTIVE RELIEF FOR A SUBSTANTIAL
19 PRIVACY HARM.—Notice is not required under para-
20 graph (1) prior to filing an action for injunctive re-
21 lief for a violation that resulted in a substantial pri-
22 vacy harm.

23 (c) NOTICE OF ACTIONS SEEKING ACTUAL DAM-
24 AGES.—

1 (1) NOTICE.—Subject to paragraph (2), an ac-
2 tion under this section for actual damages may be
3 brought by an individual only if, prior to initiating
4 such action against an entity, the individual provides
5 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) NO NOTICE REQUIRED FOR A SUBSTANTIAL
9 PRIVACY HARM.—Notice is not required under para-
10 graph (1) prior to filing an action for actual dam-
11 ages for a violation of this Act that resulted in a
12 substantial privacy harm, if such action includes a
13 claim for a preliminary injunction or temporary re-
14 straining order.

15 (d) PRE-DISPUTE ARBITRATION AGREEMENTS.—

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

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

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

1 (2) DETERMINATION OF APPLICABILITY.—Any
2 issue as to whether this section applies to a dispute
3 shall be determined under Federal law. The applica-
4 bility of this section to an agreement to arbitrate
5 and the validity and enforceability of an agreement
6 to which this section applies shall be determined by
7 a Federal court, rather than an arbitrator, irrespec-
8 tive of whether the party resisting arbitration chal-
9 lenges the arbitration agreement specifically or in
10 conjunction with other terms of the contract con-
11 taining such agreement, and irrespective of whether
12 the agreement purports to delegate such determina-
13 tion to an arbitrator.

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

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

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

24 (a) PREEMPTION OF STATE LAWS.—

1 (1) CONGRESSIONAL INTENT.—The purposes of
2 this Act are to—

3 (A) establish a uniform national privacy
4 and data security standard in the United States
5 to prevent administrative costs burdens placed
6 on interstate commerce; and

7 (B) expressly preempt laws of a State or
8 political subdivision of a State as provided in
9 this subsection.

10 (2) PREEMPTION.—Except as provided in para-
11 graph (3), no State or political subdivision of a
12 State may adopt, maintain, enforce, or continue in
13 effect any law, regulation, rule, or requirement cov-
14 ered by the provisions of this Act or a rule, regula-
15 tion, or requirement promulgated under this Act.

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

20 (A) Consumer protection laws of general
21 applicability, such as laws regulating deceptive,
22 unfair, or unconscionable practices.

23 (B) Civil rights laws.

1 (C) Provisions of laws that address the pri-
2 vacy rights or other protections of employees or
3 employee information.

4 (D) Provisions of laws that address the
5 privacy rights or other protections of students
6 or student information.

7 (E) Provisions of laws, insofar as such pro-
8 visions address notification requirements in the
9 event of a data breach.

10 (F) Contract or tort law.

11 (G) Criminal laws unrelated to data or
12 data security.

13 (H) Criminal or civil laws regarding—

14 (i) blackmail;

15 (ii) stalking (including cyberstalking),

16 (iii) cyberbullying,

17 (iv) intimate images (whether authen-

18 tic or computer-generated) known to be

19 nonconsensual,

20 (v) child abuse,

21 (vi) child sexual abuse material,

22 (vii) child abduction or attempted

23 child abduction,

24 (viii) child trafficking, or

25 (ix) sexual harassment.

1 (I) Public safety or sector spe-
2 cific laws unrelated to privacy or data
3 security, but only to the extent such
4 laws do not directly conflict with the
5 provisions of this Act.

6 (J) Provisions of laws that address public
7 records, criminal justice information systems,
8 arrest records, mug shots, conviction records, or
9 non-conviction records.

10 (K) Provisions of laws that address bank-
11 ing records, financial records, tax records, So-
12 cial Security numbers, credit cards, identity
13 theft, credit reporting and investigations, credit
14 repair, credit clinics, or check-cashing services.

15 (L) Provisions of laws that address elec-
16 tronic surveillance, wiretapping, or telephone
17 monitoring.

18 (M) Provisions of laws that address unso-
19 licited email messages, telephone solicitation, or
20 caller ID.

21 (N) Provisions of laws that protect the pri-
22 vacy of health information, healthcare informa-
23 tion, medical information, medical records, HIV
24 status, or HIV testing.

1 (O) Provisions of laws that address the
2 confidentiality of library records.

3 (P) Provisions of laws that address the use
4 of encryption as a means of providing data se-
5 curity.

6 (b) FEDERAL LAW PRESERVATION.—

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

10 (A) the authority of the Commission, or
11 any other Executive agency, under any other
12 provision of law;

13 (B) any requirement for a common carrier
14 subject to section 64.2011 of title 47, Code of
15 Federal Regulations (or any successor regula-
16 tion) regarding information security breaches;
17 or

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

20 (2) ANTITRUST SAVINGS CLAUSE.—

21 (A) ANTITRUST LAWS DEFINED.—For pur-
22 poses of this paragraph, the term “antitrust
23 laws”—

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

4 (ii) includes section 5 of the Federal
5 Trade Commission Act (15 U.S.C. 45), to
6 the extent that section applies to unfair
7 methods of competition.

8 (B) FULL APPLICATION OF THE ANTI-
9 TRUST LAWS.—Nothing in this Act or the regu-
10 latory regime created under this Act, may be
11 construed to modify, impair, supersede the op-
12 eration of, or preclude the application of the
13 antitrust laws.

14 (3) APPLICATION OF OTHER FEDERAL PRIVACY
15 REQUIREMENTS.—

16 (A) IN GENERAL.—A covered entity or
17 service provider that is required to comply with
18 the laws and regulations described in subpara-
19 graph (B) and is in compliance with the data
20 privacy requirements of such laws and regula-
21 tions shall be deemed to be in compliance with
22 the related provisions of this Act (except with
23 respect to section 9), solely and exclusively with
24 respect to any data subject to the requirements
25 of such laws and regulations.

1 (B) LAWS AND REGULATIONS DE-
2 SCRIBED.—For purposes of subparagraph (A),
3 the laws and regulations described in this sub-
4 paragraph are the following:

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

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

9 (iii) Subtitle D of the Health Informa-
10 tion Technology for Economic and Clinical
11 Health Act (42 U.S.C. 17931 et seq.).

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

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

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

24 (vii) Section 444 of the General Edu-
25 cation Provisions Act of 1974 (commonly

1 known as the “Family Educational Rights
2 and Privacy Act”) (20 U.S.C. 1232g) and
3 part 99 of title 34, Code of Federal Regu-
4 lations (or any successor regulation), to
5 the extent such covered entity or service
6 provider is an educational agency or insti-
7 tution as defined in such section of such
8 Act or section 99.3 of title 34, Code of
9 Federal Regulations (or any successor reg-
10 ulation).

11 (B) IMPLEMENTATION GUIDANCE.—Not
12 later than 1 year after the date of the enact-
13 ment of this Act, the Commission shall issue
14 guidance describing the implementation of this
15 paragraph.

16 (4) APPLICATION OF OTHER FEDERAL DATA
17 SECURITY REQUIREMENTS.—

18 (A) IN GENERAL.—A covered entity or
19 service provider that is required to comply with
20 the laws and regulations described in subpara-
21 graph (B) and is in compliance with the infor-
22 mation security requirements of such laws and
23 regulations shall be deemed to be in compliance
24 with section 9 of this Act, solely and exclusively

1 with respect to any data subject to the require-
2 ments of such laws and regulations.

3 (B) LAWS AND REGULATIONS DE-
4 SCRIBED.—For purposes of subparagraph (A),
5 the laws and regulations described in this sub-
6 paragraph are the following:

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

9 (ii) The Health Information Tech-
10 nology for Economic and Clinical Health
11 Act (42 U.S.C. 17931 et seq.).

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

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

18 (B) IMPLEMENTATION GUIDANCE.—Not
19 later than 1 year after the date of the enact-
20 ment of this Act, the Commission shall issue
21 guidance describing the implementation of this
22 paragraph.

23 (c) PRESERVATION OF COMMON LAW OR STATUTORY
24 CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this
25 Act, nor any amendment, standard, rule, requirement, as-

1 assessment, law, or regulation promulgated under this Act,
2 may be construed to preempt, displace, or supplant any
3 Federal or State common law rights or remedies, or any
4 statute creating a remedy for civil relief, including any
5 cause of action for personal injury, wrongful death, prop-
6 erty damage, or other financial, physical, reputational, or
7 psychological injury based in negligence, strict liability,
8 products liability, failure to warn, an objectively offensive
9 intrusion into the private affairs or concerns of an indi-
10 vidual, or any other legal theory of liability under any Fed-
11 eral or State common law, or any State statutory law, ex-
12 cept that the fact of a violation of this Act or a regulation
13 promulgated under this Act may not be pleaded as an ele-
14 ment of any violation of such law.

15 (d) NONAPPLICATION OF FCC PRIVACY LAWS AND
16 REGULATIONS TO CERTAIN COVERED ENTITIES.—

17 (1) IN GENERAL.—Notwithstanding any other
18 provision of law and except as provided in paragraph
19 (2), the Communications Act of 1934 (47 U.S.C.
20 151 et seq) and all Acts amendatory thereof or sup-
21 plementary thereto.), and any regulation promul-
22 gated by the Federal Communications Commission
23 under such Act, does not apply to any covered entity
24 or service provider with respect to the collection,
25 processing, retention, transfer, or security of covered

1 data to the extent that such collection, processing,
2 retention, transfer, or security of covered data is
3 governed by the requirements of this Act.

4 (2) EXCEPTIONS.—Paragraph (1) shall not pre-
5 clude the application of any of the following to a
6 covered entity or service provider with respect to the
7 collection, processing, retention, transfer, or security
8 of covered data:

9 (A) Subsections (b), (d), and (g) of section
10 222 of the Communications Act of 1934 (47
11 U.S.C. 222).

12 (B) Section 64.2011 of title 47, Code of
13 Federal Regulations (or any successor regula-
14 tion).

15 (C) Mitigation measures and actions taken
16 pursuant to Executive Order 13913 (85 Fed.
17 Reg. 19643; relating to the establishment of the
18 Committee for the Assessment of Foreign Par-
19 ticipation in the United States Telecommuni-
20 cations Services Sector).

21 (D) Any obligation under an international
22 treaty related to the exchange of traffic imple-
23 mented and enforced by the Federal Commu-
24 nications Commission.

1 **SEC. 21. CHILDRENS ONLINE PRIVACY PROTECTION ACT**
2 **OF 1998.**

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

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

9 Beginning on the date of the enactment of this Act,
10 the rulemaking proposed in the advance notice of proposed
11 rulemaking titled “Trade Regulation Rule on Commercial
12 Surveillance and Data Security” and published on August
13 8, 2022, shall be terminated.

14 **SEC. 23. SEVERABILITY.**

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

20 **SEC. 24. EFFECTIVE DATE.**

21 This Act shall take effect on the date that is 180 days
22 after the date of the enactment of this Act, unless other-
23 wise specified in this Act.