

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

2  
3

4 Be it enacted by the Senate and House of Representatives of the United States of America in  
5 Congress assembled,

## 6 SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

7 (a) Short Title.—This Act may be cited as the “American Privacy Rights Act of 2024.

8 (b) Table of Contents.—The table of contents for this Act is as follows:

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

10 Sec.2.Definitions.

11 Sec.3.Data minimization.

12 Sec.4.Transparency.

13 Sec.5.Individual control over covered data.

14 Sec.6.Opt-out rights and centralized mechanism.

15 Sec.7.Interference with consumer rights.

16 Sec.8.Prohibition on denial of service and waiver of rights.

17 Sec.9.Data security and protection of covered data.

18 Sec.10.Executive responsibility.

19 Sec.11.Service providers and third parties.

20 Sec.12.Data brokers.

21 Sec.13.Civil rights and algorithms.

22 Sec.14.Consequential decision opt out.

23 Sec.15.Commission approved compliance guidelines.

24 Sec.16.Privacy-enhancing technology pilot program.

25 Sec.17.Enforcement by the Federal Trade Commission.

26 Sec.18.Enforcement by States.

27 Sec.19.Enforcement by individuals.

28 Sec.20.Relation to other laws.

29 Sec.21.Children’s Online Privacy Protection Act of 1998.

30 Sec.22.Termination of FTC rulemaking on commercial surveillance and data security.

31 Sec.23.Severability.

32 Sec.24.Effective date.

## 33 SEC. 2. DEFINITIONS.

1 In this Act:

2 (1) AFFIRMATIVE EXPRESS CONSENT.—

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

5 (i) clearly communicates the individual’s authorization for an act or practice;

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

8 (iii) meets the requirements of subparagraph (B).

9 (B) REQUEST REQUIREMENTS.—The requirements of this subparagraph, with respect  
10 to a request made under subparagraph (A), are the following:

11 (i) The request is provided to the individual in a clear and conspicuous  
12 standalone disclosure.

13 (ii) The request includes a description of each act or practice for which the  
14 individual’s consent is sought and—

15 (I) clearly distinguishes between an act or practice which is necessary to  
16 fulfill a request of the individual and an act or practice which is for another  
17 purpose;

18 (II) clearly states the specific categories of covered data that the covered  
19 entity shall collect, process, retain, or transfer to fulfill the request; and

20 (III) is written in easy-to-understand language and includes a prominent  
21 heading that would enable a reasonable individual to identify and understand  
22 the act or practice.

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

25 (iv) The request is made in a manner reasonably accessible to and usable by  
26 individuals with disabilities.

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

29 (vi) The option to refuse consent shall be at least as prominent as the option to  
30 accept, and the option to refuse consent shall take the same number of steps or  
31 fewer as the option to accept.

32 (C) EXPRESS CONSENT REQUIRED.—Affirmative express consent to an act or practice  
33 shall not be inferred from the inaction of the individual or the individual’s continued  
34 use of a service or product provided by the covered entity.

35 (2) BIOMETRIC INFORMATION.—

36 (A) IN GENERAL.—The term “biometric information” means any covered data that is  
37 specific to an individual and is generated from the measurement or processing of the  
38 individual’s unique biological, physical, or physiological characteristics that is linked  
39 or reasonably linkable to the individual, including—

- 1 (i) fingerprints;
- 2 (ii) voice prints;
- 3 (iii) iris or retina imagery scans;
- 4 (iv) facial or hand mapping, geometry, templates; or
- 5 (v) gait.
- 6 (B) EXCLUSION.—The term “biometric information” does not include—
- 7 (i) a digital or physical photograph;
- 8 (ii) an audio or video recording; or
- 9 (iii) metadata associated with a digital or physical photograph or an audio or
- 10 video recording that cannot be used to identify an individual.
- 11 (3) COLLECT; COLLECTION.—The terms “collect” and “collection” mean buying, renting,
- 12 gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any
- 13 means.
- 14 (4) COMMISSION.—The term “Commission” means the Federal Trade Commission.
- 15 (5) COMMON BRANDING.—The term “common branding” means a name, service mark, or
- 16 trademark that is shared by 2 or more entities.
- 17 (6) CONNECTED DEVICE.—The term “connected device” means a device that is capable of
- 18 connecting to the internet over a fixed or wireless connection.
- 19 (7) CONTROL.—The term “control” means, with respect to an entity—
- 20 (A) ownership of, or the power to vote, more than 50 percent of the outstanding
- 21 shares of any class of voting security of the entity;
- 22 (B) control over the election of a majority of the directors of the entity (or of
- 23 individuals exercising similar functions); or
- 24 (C) the power to exercise a controlling influence over the management of the entity.
- 25 (8) COVERED ALGORITHM.—The term “covered algorithm” means a computational
- 26 process, including one derived from machine learning, statistics, or other data processing or
- 27 artificial intelligence techniques, that makes a decision or facilitates human decision-
- 28 making by using covered data, which includes determining the provision of products or
- 29 services or ranking, ordering, promoting, recommending, amplifying, or similarly
- 30 determining the delivery or display of information to an individual.
- 31 (9) COVERED DATA.—
- 32 (A) IN GENERAL.—The term “covered data” means information that identifies or is
- 33 linked or reasonably linkable, alone or in combination with other information, to an
- 34 individual or a device that identifies or is linked or reasonably linkable to 1 or more
- 35 individuals.
- 36 (B) EXCLUSIONS.—The term “covered data” does not include—
- 37 (i) de-identified data;

- 1 (ii) employee information;
- 2 (iii) publicly available information;
- 3 (iv) inferences made exclusively from multiple independent sources of publicly  
4 available information provided that such inferences—
  - 5 (I) do not reveal information about an individual that meets the definition  
6 of sensitive covered data with respect to an individual; and
  - 7 (II) are not combined with covered data; or
- 8 (v) information in the collection of a library, archive, or museum if the library,  
9 archive, or museum has—
  - 10 (I) a collection that is open to the public or routinely made available to  
11 researchers who are not affiliated with the library, archive, or museum;
  - 12 (II) a public service mission;
  - 13 (III) trained staff or volunteers to provide professional services normally  
14 associated with libraries, archives, or museums; and
  - 15 (IV) collections composed of lawfully acquired materials and all licensing  
16 conditions for such materials are met.

17 (10) COVERED ENTITY.—

18 (A) IN GENERAL.—The term “covered entity”—

- 19 (i) means any entity that, alone or jointly with others, determines the purposes  
20 and means of collecting, processing, retaining, or transferring covered data and—
  - 21 (I) is subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.);
  - 22 (II) is a common carrier subject to title II of the Communications Act of  
23 1934 (47 U.S.C. 201–231) as currently enacted or subsequently amended; or
  - 24 (III) is an organization not organized to carry on business for their own  
25 profit or that of their members;
- 26 (ii) includes any entity that controls, is controlled by, is under common control  
27 with, or shares common branding with another covered entity; and
- 28 (iii) does not include—
  - 29 (I) a Federal, State, Tribal, territorial, or local government entity such as a  
30 body, authority, board, bureau, commission, district, agency, or political  
31 subdivision of the Federal Government or a State, Tribal, territorial, or local  
32 government;
  - 33 (II) an entity that is collecting, processing, retaining, or transferring  
34 covered data on behalf of a Federal, State, Tribal, territorial, or local  
35 government entity, to the extent that such entity is acting as a service  
36 provider to the government entity;
  - 37 (III) a small business;

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

2 (V) except with respect to the obligations under section 9, a nonprofit  
3 organization whose primary mission is to prevent, investigate, or deter fraud  
4 or to train anti-fraud professionals or educate the public about fraud,  
5 including insurance fraud, securities fraud, and financial fraud to the extent  
6 the organization collects, processes, retains, or transfers covered data in  
7 furtherance of such primary mission.

8 (B) NONAPPLICATION TO SERVICE PROVIDERS.—An entity shall not be considered to  
9 be a “covered entity” for the purposes of this Act, insofar as the entity is acting as a  
10 service provider.

11 (11) COVERED HIGH-IMPACT SOCIAL MEDIA COMPANY.—The term “covered high-impact  
12 social media company” means a covered entity that provides any internet-accessible  
13 platform where—

14 (A) such covered entity generates \$3,000,000,000 or more in global annual revenue,  
15 including the revenue generated by any affiliate of such covered entity;

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

18 (C) such platform constitutes an online product or service that is primarily used by  
19 individuals to access or share user-generated content.

20 (12) COVERED MINOR.—The term “covered minor” means an individual under the age of  
21 17.

22 (13) DATA BROKER.—

23 (A) IN GENERAL.—The term “data broker” means a covered entity whose principal  
24 source of revenue is derived from processing or transferring covered data that the  
25 covered entity did not collect directly from the individuals linked or linkable to such  
26 covered data.

27 (B) PRINCIPAL SOURCE OF REVENUE DEFINED.—For purposes of this paragraph, the  
28 term “principal source of revenue” means, with respect to the preceding 12-month  
29 period—

30 (i) revenue that constitutes greater than 50 percent of all revenue of the covered  
31 entity during such period; or

32 (ii) revenue obtained from processing or transferring the covered data of more  
33 than 5,000,000 individuals that the covered entity did not collect directly from the  
34 individuals linked or linkable to the covered data.

35 (C) NON-APPLICATION TO SERVICE PROVIDERS.—The term “data broker” does not  
36 include an entity to the extent that such entity is acting as a service provider.

37 (14) DARK PATTERNS.—The term “dark patterns” means a user interface designed or  
38 manipulated with the substantial effect of subverting or impairing user autonomy, decision  
39 making, or choice.

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

1 (A) information that cannot reasonably be used to infer or derive the identity of an  
2 individual, does not identify and is not linked or reasonably linkable to an individual or  
3 a device that identifies or is linked or reasonably linkable to such individual, regardless  
4 of whether the information is aggregated, provided that the covered entity or service  
5 provider—

6 (i) takes reasonable physical, administrative, or technical measures to ensure  
7 that the information cannot, at any point, be used to re-identify any individual or  
8 device that identifies or is linked or reasonably linkable to an individual;

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

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

12 (II) not attempt to re-identify the information with any individual or  
13 device that identifies or is linked or reasonably linkable to an individual; and

14 (iii) contractually obligates any entity that receives the information from the  
15 covered entity or service provider to—

16 (I) comply with all of the provisions of this paragraph with respect to the  
17 information; and

18 (II) require that such contractual obligations be included in all subsequent  
19 instances for which the data may be received; or

20 (B) health information (as defined in section 262 of the Health Insurance Portability  
21 and Accountability Act of 1996 (42 U.S.C. 1320d)) that has been de-identified in  
22 accordance with section 164.514(b) of title 45, Code of Federal Regulations, provided  
23 that if such information is subsequently provided to an entity that is not an entity  
24 subject to parts 160 and 164 of such title 45, such entity must comply with clauses (ii)  
25 and (iii) of subparagraph (A) for the information to be considered de-identified under  
26 this Act.

27 (16) DERIVED DATA.—The term “derived data” means covered data that is created by the  
28 derivation of information, data, assumptions, correlations, inferences, predictions, or  
29 conclusions from facts, evidence, or another source of information or data about an  
30 individual or an individual’s device.

31 (17) DEVICE.—The term “device” means any electronic equipment capable of collecting,  
32 processing, retaining, or transferring covered data that is used by one or more individuals,  
33 including a connected device or a portable connected device.

34 (18) EMPLOYEE.—The term “employee” means an individual who is an employee,  
35 director, officer, staff member, or individual working as an independent contractor that is  
36 not a service provider, volunteer, or intern of an employer, regardless of whether such  
37 individual is paid, unpaid, or employed on a temporary basis.

38 (19) EMPLOYEE INFORMATION.—The term “employee information” means covered data,  
39 biometric information, or genetic information that is collected by a covered entity (or a  
40 service provider acting on behalf of a covered entity)—

41 (A) about an individual in the course of the individual’s employment or application

1 for employment (including on a contract or temporary basis), provided that such data is  
2 retained or processed by the covered entity or the service provider solely for purposes  
3 necessary for the individual’s employment or application for employment;

4 (B) that is emergency contact information for an individual who is an employee or  
5 job applicant of the covered entity, provided that such data is retained or processed by  
6 the covered entity or the service provider solely for the purpose of having an  
7 emergency contact for such individual on file; or

8 (C) about an individual (or a relative of an individual) who is an employee or former  
9 employee of the covered entity for the purpose of administering benefits to which such  
10 individual or relative is entitled on the basis of the individual’s employment with the  
11 covered entity, provided that such data is retained or processed by the covered entity or  
12 the service provider solely for the purpose of administering such benefits.

13 (20) ENTITY.—The term “entity” means an individual, trust, partnership, association,  
14 organization, company, or corporation.

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

17 (22) GENETIC INFORMATION.—The term “genetic information” means any covered data,  
18 regardless of its format, that concerns an identified or identifiable individual’s genetic  
19 characteristics, including—

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

22 (B) genotypic and phenotypic information that results from analyzing raw sequence  
23 data described in subparagraph (A).

24 (23) HEALTH INFORMATION.—The term “health information” means information that  
25 describes or reveals the past, present, or future physical health, mental health, disability,  
26 diagnosis, or health condition or treatment of an individual, including the precise  
27 geolocation information of such treatment.

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

30 (25) LARGE DATA HOLDER.—

31 (A) IN GENERAL.—The term “large data holder” means a covered entity or service  
32 provider that, in the most recent calendar year had an annual gross revenue of not less  
33 than \$250,000,000 and, subject to subparagraph (B), collected, processed, retained, or  
34 transferred—

35 (i) the covered data of—

36 (I) more than 5,000,000 individuals;

37 (II) 15,000,000 portable connected devices that identify or are linked or  
38 reasonably linkable to 1 or more individuals; and

39 (III) 35,000,000 connected devices that identify or are linked or reasonable  
40 linkable to 1 or more individuals; or

1 (ii) the sensitive covered data of—

2 (I) more than 200,000 individuals;

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

5 (III) 700,000 connected devices that identify or are linked or reasonably  
6 linkable to 1 or more individuals.

7 (B) EXCLUSIONS.—For purposes of subparagraph (A), a covered entity or service  
8 provider shall not be considered a large data holder solely on account of collecting,  
9 processing, retaining, or transferring to a service provider—

10 (i) personal mailing or email addresses;

11 (ii) personal telephone numbers;

12 (iii) log-in information of an individual or device to allow the individual or  
13 device to log in to an account administered by the covered entity; or

14 (iv) in the case of a covered entity that is a seller of goods or services (other  
15 than an entity that facilitates payment, such as a bank, credit card processor,  
16 mobile payment system, or payment platform), credit, debit, or mobile payment  
17 information strictly necessary to initiate, render, bill for, finalize, complete, or  
18 otherwise facilitate payments for goods or services.

19 (C) DEFINITION OF ANNUAL GROSS REVENUE.—For purposes of subparagraph (A),  
20 the term “annual gross revenue”, with respect to a covered entity or service provider—

21 (i) means the gross receipts the covered entity or service provider received, in  
22 whatever form from all sources, without subtracting any costs or expenses; and

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

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

29 (A) integrated into any product or service;

30 (B) otherwise used to contact any individual or individual’s device; or

31 (C) used for targeted advertising or to otherwise market to any individual or  
32 individual’s device.

33 (27) MATERIAL CHANGE.—The term “material change” means, with respect to treatment  
34 of covered data, a change by an entity that would likely affect an individual’s decision to  
35 provide affirmative express consent for, or opt out of, the entity’s collection, processing,  
36 retention, or transfer of covered data pertaining to such individual.

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



1 (29) PORTABLE CONNECTED DEVICE.—The term “portable connected device” means a  
2 portable device that is capable of connecting to the internet over a wireless connection,  
3 including a smartphone, tablet computer, laptop computer, smartwatch, or similar portable  
4 device.

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

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

9 (B) the location of such individual or device within a range of 1,850 feet or less.

10 (31) PROCESS.—The term “process” means any operation or set of operations performed  
11 on covered data, including analyzing, organizing, structuring, using, modifying, or  
12 otherwise handling covered data.

13 (32) PUBLICLY AVAILABLE INFORMATION.—

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

17 (i) Federal, State, or local government records provided that the covered entity  
18 collects, processes, retains, and transfers such information in accordance with any  
19 restrictions or terms of use placed on the information by the relevant government  
20 entity;

21 (ii) widely distributed media;

22 (iii) a website or online service made available to all members of the public, for  
23 free or for a fee, including where all members of the public can log-in to the  
24 website or online service; or

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

27 (B) CLARIFICATIONS; LIMITATIONS.—

28 (i) AVAILABLE TO ALL MEMBERS OF THE PUBLIC.—For purposes of this  
29 paragraph, information from a website or online service is not available to all  
30 members of the public if the individual to whom the information pertains has  
31 restricted the information to a specific audience.

32 (ii) BUSINESS CONTACT INFORMATION.—The term “publicly available  
33 information” includes the business contact information of an employee that is  
34 made available to all members of the public on a website or online service,  
35 including the employee’s name, position or title, business telephone number,  
36 business email address, or address.

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

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

1 (II) Derived data from publicly available information that reveals  
2 information about an individual that meets the definition of sensitive covered  
3 data.

4 (III) Biometric information.

5 (IV) Genetic information.

6 (V) Covered data that has been combined with publicly available  
7 information.

8 (VI) Intimate images, authentic or generated by a computer or by artificial  
9 intelligence, known to be nonconsensual.

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

12 (34) SENSITIVE COVERED DATA.—

13 (A) IN GENERAL.—The term “sensitive covered data” means the following forms of  
14 covered data:

15 (i) A government-issued identifier, such as a social security number, passport  
16 number, or driver’s license number, that is not required by law to be displayed in  
17 public.

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

21 (iii) Genetic Information.

22 (iv) A financial account number, debit card number, credit card number, or any  
23 required security or access code, password, or credentials allowing access to any  
24 such account or card.

25 (v) Biometric information.

26 (vi) Precise geolocation information.

27 (vii) An individual’s private communications, such as voicemails, emails, texts,  
28 direct messages, or mail, or information identifying the parties to such  
29 communications, information contained in telephone bills, voice communications,  
30 and any information that pertains to the transmission of voice communications,  
31 including numbers called, numbers from which calls were placed, the time calls  
32 were made, call duration, and location information of the parties to the call, unless  
33 the covered entity is an intended recipient of the communication.

34 (viii) Account or device log-in credentials.

35 (ix) Information revealing the sexual behavior of an individual in a manner  
36 inconsistent with the individual’s reasonable expectation regarding disclosure of  
37 such information.

38 (x) Calendar information, address book information, phone or text logs, photos,  
39 audio recordings, or videos intended for private use.

1 (xi) A photograph, film, video recording, or other similar medium that shows  
2 the naked or undergarment-clad private area of an individual.

3 (xii) Information revealing the extent or content of any individual’s access,  
4 viewing, or other use of any video programming described in section 713(b)(2) of  
5 the Communications Act of 1934 (47 U.S.C. 613(h)(2)), including by a provider  
6 of broadcast television service, cable service, satellite service, or streaming media  
7 service, but only with regard to the transfer of such information to a third party  
8 (excluding any such data used solely for transfers for independent video  
9 measurement).

10 (xiii) Information collected by a covered entity that is not a provider of a  
11 service described in clause (xii) that reveals the video content requested or  
12 selected by an individual (excluding any such data used solely for transfers for  
13 independent video measurement).

14 (xiv) Information revealing an individual’s race, ethnicity, national origin,  
15 religion, or sex in a manner inconsistent with the individual’s reasonable  
16 expectation regarding disclosure of such information.

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

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

22 (xvii) Any other covered data collected, processed, retained, or transferred for  
23 the purpose of identifying the data types described in clauses (i) through (xvi).

24 (xviii) Any other covered data, except for expanding the categories described in  
25 clause (ii), that the Commission determines to be sensitive covered data through a  
26 rulemaking pursuant to section 553 of title 5, United States Code.

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

29 (i) is related by common ownership or corporate control to the provider of  
30 broadcast television service, cable service, satellite service, or streaming media  
31 service; and

32 (ii) provides video programming as described in subparagraph (A)(xii).

33 (35) SERVICE PROVIDER.—

34 (A) IN GENERAL.—The term “service provider” means an entity that collects,  
35 processes, retains, or transfers covered data for the purpose of performing 1 or more  
36 services or functions on behalf of, and at the direction of, a covered entity.

37 (B) RULE OF CONSTRUCTION.—

38 (i) IN GENERAL.—An entity is a “covered entity” and not a “service provider”  
39 with respect to a specific collecting, processing, retaining, or transferring of data  
40 if the entity, jointly or with others, determines the purposes and means of the

1 specific collecting, processing, retaining, or transferring of data.

2 (ii) CONTEXT REQUIRED.—Whether an entity is a “covered entity” or a “service  
3 provider” depends on the facts surrounding, and the context in which, the data is  
4 collected, processed, retained, or transferred.

5 (36) SMALL BUSINESS.—

6 (A) IN GENERAL.—The term “small business” means an entity (including any  
7 affiliate of the entity)—

8 (i) whose average annual gross revenues for the period of the 3 preceding  
9 calendar years (or for the period during which the covered entity has been in  
10 existence if such period is less than 3 years) did not exceed \$40,000,000;

11 (ii) that, on average, did not annually collect, process, retain, or transfer the  
12 covered data of more than 200,000 individuals for any purpose other than  
13 initiating, rendering, billing for, finalizing, completing, or otherwise collecting  
14 payment for a requested service or product, so long as all covered data for such  
15 purpose was deleted or de-identified within 90 days, except when necessary to  
16 investigate fraud or as consistent with a covered entity’s return or warranty  
17 policy; and

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

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

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

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

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

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

32 (i) treatment by a licensed, credentialed, or otherwise bona fide health care  
33 provider, hospital, community health center, clinic, hospice, or residential or  
34 outpatient facility for medical, mental health, or addiction care; or

35 (ii) physical injury, highly offensive intrusion into the privacy expectations of a  
36 reasonable individual under the circumstances, or discrimination on the basis of  
37 race, color, religion, national origin, sex, or disability.

38 (39) TARGETED ADVERTISING.—The term “targeted advertising”—

39 (A) means displaying or presenting to an individual or device identified by a unique  
40 persistent identifier (or group of individuals or devices identified by unique persistent

1 identifiers) an online advertisement that is selected based on known or predicted  
2 preferences or interests associated with the individual or device identified by a unique  
3 identifier; and

4 (B) does not include—

5 (i) advertising or marketing content to an individual in response to the  
6 individual’s specific request for information or feedback;

7 (ii) first-party advertising based on an individual’s visit to or use of a website or  
8 online service that offers a product or service that is related to the subject of the  
9 advertisement;

10 (iii) contextual advertising when an advertisement is displayed online based on  
11 the content of the webpage or online service on which the advertisement appears;  
12 or

13 (iv) processing covered data solely for measuring or reporting advertising,  
14 marketing, or media performance, reach, or frequency, including by independent  
15 entities.

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

17 (A) means any entity that—

18 (i) receives covered data from another entity; and

19 (ii) is not a service provider with respect to such data; and

20 (B) does not include an entity that collects covered data from another entity if the 2  
21 entities are related by common ownership or corporate control and share common  
22 branding.

23 (41) THIRD-PARTY DATA.—The term “third party data” means covered data that has been  
24 transferred to a third party.

25 (42) TRANSFER.—The term “transfer” means to disclose, release, share, disseminate,  
26 make available, sell, rent, or license covered data, orally, in writing, electronically, or by  
27 any other means for consideration of any kind or for a commercial purpose.

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

29 (A) a technologically created identifier to the extent that such identifier is reasonably  
30 linkable to an individual or device that identifies or is linked or reasonably linkable to  
31 1 or more individuals, including a device identifier, an Internet Protocol address,  
32 cookies, beacons, pixel tags, mobile ad identifiers, or similar technology, customer  
33 number, unique pseudonym, or user alias, telephone numbers, or other forms of  
34 persistent or probabilistic identifiers that are linked or reasonably linkable to 1 or more  
35 individuals or devices; and

36 (B) does not include an identifier assigned by a covered entity for the specific  
37 purpose of giving effect to an individual’s exercise of affirmative express consent or  
38 opt-out of the collection, processing, retaining, or transfer of covered data or otherwise  
39 limiting the collection, processing, retaining, or transfer of such information.

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

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

5 (B) does not include an obscene visual depiction (as defined in section 1460 of title  
6 18, United States Code).

### 7 SEC. 3. DATA MINIMIZATION.

8 (a) In General.—Subject to subsections (b) and (c), a covered entity, or a service provider  
9 acting on behalf of a covered entity, shall not collect, process, retain, or transfer covered data—

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

11 (A) a specific product or service requested by the individual to whom the data  
12 pertains, including any associated routine administrative, operational, or account-  
13 servicing activity such as billing, shipping, delivery, storage, or accounting; or

14 (B) a communication by the covered entity to the individual reasonably anticipated  
15 within the context of the relationship; or

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

17 (b) Sensitive Covered Data.—

18 (1) IN GENERAL.—Except as expressly provided under subsection (d), a covered entity, or  
19 a service provider acting on behalf of a covered entity, shall not transfer sensitive covered  
20 data to a third party without the affirmative express consent of the individual to whom such  
21 data pertains.

22 (2) WITHDRAWAL OF AFFIRMATIVE EXPRESS CONSENT.—

23 (A) IN GENERAL.—A covered entity shall provide an individual with a means to  
24 withdraw affirmative express consent previously provided by the individual with  
25 respect to the transfer of the sensitive covered data of the individual.

26 (B) REQUIREMENTS.—The means to withdraw affirmative express consent described  
27 in subparagraph (A) shall be—

28 (i) clear and conspicuous; and

29 (ii) as easy for a reasonable individual to use as the mechanism by which the  
30 individual provided affirmative express consent.

31 (c) Additional Protections for Biometric Information and Genetic Information.—

32 (1) IN GENERAL.—A covered entity, or a service provider acting on behalf of a covered  
33 entity, shall not collect, process, or retain biometric information or genetic information  
34 without the affirmative express consent of the individual to whom such information  
35 pertains, unless such collection, processing, or retention is essential for a purpose expressly  
36 permitted under paragraphs (1) through (4) or paragraphs (9) through (13) of subsection (d).

37 (2) RETENTION.—A covered entity, or service provider acting on behalf of a covered  
38 entity, shall not retain biometric or genetic information beyond the point for which a  
39 purpose that an individual provided affirmative express consent under paragraph (1) has

1 been satisfied or within 3 years of the individual’s last interaction with the covered entity or  
2 service provider, whichever occurs first, unless such retention is essential for a purpose  
3 expressly permitted under paragraphs (1) through (4) or paragraphs (9) through (13) of  
4 subsection (d).

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

10 (4) WITHDRAWAL OF AFFIRMATIVE EXPRESS CONSENT.—

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

14 (B) REQUIREMENTS.—The means to withdraw affirmative express consent described  
15 in subparagraph (A) shall be—

16 (i) clear and conspicuous; and

17 (ii) as easy for a reasonable individual to use as the mechanism by which the  
18 individual provided affirmative express consent.

19 (d) Permitted Purposes.—A covered entity, or service provider acting on behalf of a covered  
20 entity, may collect, process, retain, or transfer covered data for the following purposes, provided  
21 that the covered entity or service provider can demonstrate that the collection, processing,  
22 retention, or transferring is necessary, proportionate, and limited to such purpose:

23 (1) To protect data security (as described in section 9), protect against spam, and maintain  
24 networks and systems, including through diagnostics, debugging, and repairs.

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

27 (3) To investigate, establish, prepare for, exercise, or defend cognizable legal claims on  
28 its own behalf.

29 (4) To transfer covered data to a Federal, State, local, or Tribal law enforcement agency  
30 pursuant to a lawful warrant, administrative subpoena, or other form of lawful process.

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

32 (6) To conduct market research.

33 (7) With respect to covered data previously collected in accordance with this Act, to  
34 process such data into de-identified data, including to—

35 (A) develop or enhance a product or service of the covered entity;

36 (B) conduct internal research or analytics to improve a product or service of the  
37 covered entity; or

38 (C) conduct a public or peer-reviewed scientific, historical, or statistical research  
39 project that—

1 (i) is in the public interest; and

2 (ii) adheres to all relevant laws and regulations governing such research,  
3 including regulations for the protection of human subjects.

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

8 (A) a notice describing such transfer, including the name of any entity receiving the  
9 individual's covered data and the privacy policies of such entity (as described in  
10 section 4); and

11 (B) a reasonable opportunity to—

12 (i) withdraw any previously given consent in accordance with the requirements  
13 of affirmative express consent under this Act related to the individual's covered  
14 data; and

15 (ii) request the deletion of the individual's covered data, as described in section  
16 5.

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

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

26 (11) To prevent, detect, protect against, or respond to an ongoing or imminent network  
27 security or physical security incident, including an intrusion or trespass, medical alerts, fire  
28 alarms, or access control.

29 (12) To prevent, detect, protect against, or respond to an imminent or ongoing public  
30 safety incident (such a mass casualty event, natural disaster, or national security incident),  
31 excluding the transfer of covered data for payment or other valuable consideration to a  
32 government entity.

33 (13) Except with respect to health information, to prevent, detect, protect against,  
34 investigate, or respond to criminal activity, excluding the transfer of covered data for  
35 payment or other valuable consideration to a government entity.

36 (14) Except with respect to sensitive covered data and only with respect to covered data  
37 previously collected in accordance with this Act, to process such data as necessary to  
38 provide first party or contextual advertising by the covered entity for individuals.

39 (15) Except with respect to sensitive covered data and only with respect to covered data  
40 previously collected in accordance with this Act, for an individual who has not opted out of  
41 targeted advertising pursuant to section 6, to process or transfer covered data to provide



1 targeted advertising.

2 (e) Guidance.—The Commission shall issue guidance regarding what is reasonably necessary  
3 and proportionate to comply with this section.

4 (f) Journalism.—Nothing in this Act shall be construed to limit or diminish First Amendment  
5 freedoms guaranteed under the Constitution.

## 6 SEC. 4. TRANSPARENCY.

7 (a) In General.—Each covered entity and service provider shall make publicly available, in a  
8 clear, conspicuous, not misleading, easy-to-read, and readily accessible manner, a privacy policy  
9 that provides a detailed and accurate representation of the covered entity or service provider’s  
10 data collection, processing, retention, and transfer activities.

11 (b) Content of Privacy Policy.—The privacy policy required under subsection (a) shall  
12 include, at a minimum, the following:

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

14 (A) the covered entity or service provider to which the privacy policy applies  
15 (including the point of contact and a monitored email address, as applicable, for data  
16 privacy and data security inquiries); and

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

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

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

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

24 (A) the categories of covered data the covered entity or service provider collects,  
25 processes, or retains; and

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

27 (3) Whether the covered entity or service provider transfers covered data and, if so—

28 (A) each category of service provider or third party to which the covered entity or  
29 service provider transfers covered data;

30 (B) the name of each data broker to which the covered entity or service provider  
31 transfers covered data; and

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

33 (4) The length of time the covered entity or service provider intends to retain each  
34 category of covered data, including sensitive covered data, or, if it is not possible to identify  
35 that time frame, the criteria used to determine the length of time the covered entity or  
36 service provider intends to retain categories of covered data.

37 (5) A prominent description of how an individual can exercise the rights described in  
38 sections 5 and 6.

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

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

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

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

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

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

12 (d) Accessibility.—The covered entity or service provider shall provide the disclosures under  
13 this section in a manner that is reasonably accessible to and usable by individuals with  
14 disabilities.

15 (e) Material Changes.—

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

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

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

20 (ii) a means to opt out of the processing or transfer of such previously collected  
21 covered data pursuant to such material change; and

22 (B) with respect to the covered data of any individual who opts out using the means  
23 described in subparagraph (A)(ii), discontinue the processing or transfer of such  
24 previously collected covered data, except if such processing or transfer is strictly  
25 necessary to provide a product or service specifically requested by the individual.

26 (2) DIRECT NOTIFICATION.—The covered entity shall take all reasonable electronic  
27 measures to provide direct notification, where possible, to each affected individual  
28 regarding material changes to the privacy policy, and such notification shall be provided in  
29 each language in which the privacy policy is made available, taking into account available  
30 technology and the nature of the relationship.

31 (3) CLARIFICATION.—Except as provided in paragraph (1)(B), nothing in this section  
32 shall be construed to affect the requirements for covered entities under section 3, 5, or 6.

33 (f) Transparency Requirements for Large Data Holders.—

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

36 (A) retain and publish on the website of the large data holder a copy of each  
37 previous version of its privacy policy (as described in subsection (d)) for not less than  
38 10 years; and

39 (B) make publicly available on its website, in a clear, conspicuous, and readily

1 accessible manner, a log that describes the date and nature of each material change to  
2 its privacy policy during such 10-year period in a manner that is sufficient for a  
3 reasonable individual to understand the effect of each material change.

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

5 (A) IN GENERAL.—In addition to the privacy policy required under subsection (a), a  
6 large data holder shall provide a short-form notice of its covered data practices in a  
7 manner that—

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

9 (ii) is readily accessible to the individual, based on the way an individual  
10 interacts with the large data holder and its products or services and what is  
11 reasonably anticipated within the context of the relationship between the  
12 individual and the large data holder;

13 (iii) includes an overview of individual rights and disclosures to reasonably  
14 draw attention to data practices that may be unexpected or that involve sensitive  
15 covered data; and

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

17 (B) GUIDANCE.—Not later than 180 days after the date of enactment of this Act, the  
18 Commission shall issue guidance establishing the minimum data disclosures necessary  
19 for the short-form notice described in this paragraph and shall include templates or  
20 models for such notice.

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

22 (a) Access to, and Correction, Deletion, and Portability of, Covered Data.—Subject to  
23 subsections (b), (d), and (e), after receiving a verified request from an individual, a covered  
24 entity shall provide the individual with the right to—

25 (1) access—

26 (A) in a format that be naturally read by a human, the covered data of the individual  
27 (or an accurate representation of the covered data of the individual if the covered data  
28 is no longer in the possession of the covered entity or a service provider acting on  
29 behalf of the covered entity) that is collected, processed, or retained by the covered  
30 entity or any service provider of the covered entity;

31 (B) the name of any third party or service provider to whom the covered entity has  
32 transferred the covered data of the individual, as well as the categories of sources from  
33 which the covered data was collected; and

34 (C) a description of the purpose for which the covered entity transferred the covered  
35 data of the individual to a third party or service provider;

36 (2) correct any inaccuracy or incomplete information with respect to the covered data of  
37 the individual that is collected, processed, or retained by the covered entity and, for covered  
38 data that has been transferred, notify any third party or service provider to which the  
39 covered entity transferred such covered data of the corrected information;

1 (3) delete covered data of the individual that is collected, processed, or retained by the  
2 covered entity and, for covered data that has been transferred, request that the covered entity  
3 notify any third party or service provider to which the covered entity transferred such  
4 covered data of the individual's deletion request; and

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

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

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

11 (b) Frequency and Cost.—A covered entity—

12 (1) shall provide an individual with the opportunity to exercise each of the rights  
13 described in subsection (a); and

14 (2) with respect to—

15 (A) the first 3 times that an individual exercises any right described in subsection (a)  
16 during any 12-month period, shall allow the individual to exercise such right free of  
17 charge; and

18 (B) any time beyond the initial 3 times described in subparagraph (A), may charge a  
19 reasonable fee for each additional request to exercise any such right during such 12-  
20 month period.

21 (c) Timing.—

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

23 (A) any large data holder or data broker shall comply with a verified request from an  
24 individual to exercise a right described in subsection (a) not later than 15 calendar days  
25 after receiving such request, unless it is impossible or demonstrably impracticable to  
26 verify such individual; and

27 (B) a covered entity that is not a large data holder shall comply with a verified  
28 request from an individual to exercise a right described in subsection (a) not later than  
29 30 calendar days after receiving such request, unless it is impossible or demonstrably  
30 impracticable to verify such individual.

31 (2) EXTENSION.—The response period required under paragraph (1) may be extended  
32 once by not more than the applicable time period described in such paragraph when  
33 reasonably necessary, considering the complexity and number of the individual's requests,  
34 provided that the covered entity informs the individual of any such extension within the  
35 initial response period, together with the reason for the extension.

36 (d) Verification.—

37 (1) IN GENERAL.—A covered entity shall verify that any individual requesting to exercise  
38 a right described in subsection (a) is—

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

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

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

4 (A) may request that the individual making such request provide any additional  
5 information necessary for the sole purpose of verifying the identity of the individual;  
6 and

7 (B) shall not process, retain, or transfer such additional information for any other  
8 purpose.

9 (e) Exceptions.—

10 (1) REQUIRED EXCEPTIONS.—A covered entity shall not permit an individual to exercise a  
11 right described in subsection (a), in whole or in part, if the covered entity—

12 (A) cannot verify that the individual making such request is the individual whose  
13 covered data is the subject of the request or an individual authorized to make such a  
14 request on the individual’s behalf;

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

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

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

23 (E) would violate the covered entity’s professional ethical obligations;

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

25 (G) except with respect to health information, reasonably believes that the request is  
26 made in furtherance of criminal activity; or

27 (H) reasonably believes that complying with the request would threaten data  
28 security.

29 (2) PERMISSIVE EXCEPTIONS.—

30 (A) IN GENERAL.—A covered entity may decline, with adequate explanation  
31 provided to the individual making the request, to comply with a request to exercise a  
32 right described in subsection (a), in whole or in part, if such compliance would—

33 (i) be demonstrably impossible due to technology or cost, and such adequate  
34 explanation includes a detailed description regarding the inability to comply with  
35 the request due to technology or cost;

36 (ii) delete covered data reasonably necessary to perform a contract between the  
37 covered entity and the individual;

38 (iii) with respect to a right described in paragraph (1) or (4) of subsection (a),  
39 require the covered entity to release trade secrets or other privileged, proprietary,

1 or confidential business information;

2 (iv) prevent a covered entity from being able to maintain a confidential record  
3 of opt out requests pursuant to section 6, maintained solely for the purpose of  
4 preventing the covered data of an individual from being recollected after the  
5 individual submitted an opt out request; or

6 (v) with respect to deletion requests, require a private elementary or secondary  
7 school (as defined by State law) or a private institution of higher education (as  
8 defined by section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)) to  
9 delete covered data that would unreasonably interfere with the provision of  
10 education services by or the ordinary operation of the school or institution.

11 (B) PARTIAL COMPLIANCE.—In the event a covered entity makes a permissive  
12 exception under subparagraph (A), the covered entity shall partially comply with the  
13 remainder of the applicable request if partial compliance is possible and not unduly  
14 burdensome.

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

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

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

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

23 (C) collect or retain any data in order to be capable of associating a verified  
24 individual's request with the covered data that is the subject of the request.

25 (4) ADDITIONAL EXCEPTIONS.—

26 (A) IN GENERAL.—The Commission may promulgate regulations, in accordance  
27 with section 553 of title 5, United States Code, to establish additional permissive  
28 exceptions necessary to protect the rights of individuals, alleviate undue burdens on  
29 covered entities, prevent unjust or unreasonable outcomes from the exercise of access,  
30 correction, deletion, or portability rights, or as otherwise necessary to fulfill the  
31 purposes of this section.

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

35 (C) CLARIFICATION.—A covered entity may not comply with an individual's request  
36 to exercise a right under this section for any purpose the Commission identifies  
37 pursuant to this paragraph.

38 (5) ON-DEVICE DATA EXEMPTION.—A covered entity may decline to comply with a  
39 request to exercise a right described in paragraph (1), (2), or (3) of subsection (a), in whole  
40 or in part, if—

1 (A) the covered data is exclusively on-device data; and

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

4 (f) Large Data Holder Metrics Reporting.—With respect to each calendar year for which an  
5 entity is considered a large data holder, such entity shall comply with the following reporting  
6 requirements:

7 (1) REQUIRED METRICS.—Compile the following metrics for the prior calendar year:

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

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

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

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

13 (E) For each category of requests described in subparagraphs (A) through (D), the  
14 number of such requests that the large data holder complied with in whole or in part.

15 (F) For each category of requests described in subparagraphs (A) through (D), the  
16 average number of days within which such large data holder substantively responded  
17 to the request.

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

20 (A) in such large data holder’s privacy policy; or

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

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

26 (h) Accessibility.—

27 (1) LANGUAGE.—A covered entity shall facilitate the ability of individuals to make  
28 requests under subsection (a) in any language in which the covered entity provides a  
29 product or service.

30 (2) INDIVIDUALS WITH DISABILITIES.—The mechanisms by which a covered entity enables  
31 individuals to make requests under subsection (a) shall be readily accessible and usable by  
32 individuals with disabilities.

## 33 SEC. 6. OPT-OUT RIGHTS AND CENTRALIZED 34 MECHANISM.

35 (a) In General.—Beginning on the effective date described in section 24, a covered entity shall  
36 provide to individuals the following opt-out rights:

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

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

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

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

8 (2) RIGHT TO OPT OUT OF TARGETED ADVERTISING.—A covered entity that engages in  
9 targeted advertising shall—

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

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

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

16 (b) Centralized Consent and Opt-out Mechanism.—

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

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

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

27 (ii) does not require that the individual provide additional information beyond  
28 what is reasonably necessary to indicate such preference;

29 (iii) clearly represents an individual’s preference and is free of defaults  
30 constraining or presupposing such preference;

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

33 (v) is provided in a manner that is reasonably accessible to and usable by  
34 individuals with disabilities; and

35 (vi) does not conflict with other commonly-used privacy settings or tools that  
36 an individual may employ;

37 (B) provides a mechanism for the individual to selectively opt out of the covered  
38 entity’s collection, processing, retention, or transfer of covered data, without affecting  
39 the individual’s preferences with respect to other entities or disabling the opt-out  
40 preference signal globally;



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

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

5 (2) EFFECT OF DESIGNATIONS.—A covered entity shall abide by any designation made by  
6 an individual through any mechanism that meets the requirements and technical  
7 specifications promulgated under paragraph (1).

## 8 SEC. 7. INTERFERENCE WITH CONSUMER RIGHTS.

9 (a) Dark Patterns Prohibited.—

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

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

12 (B) impair an individual’s ability to exercise any right under this Act; or

13 (C) obtain, infer, or facilitate an individual’s consent for any action that requires an  
14 individual’s consent under this Act.

15 (2) CLARIFICATION.—Any agreement by an individual that is obtained, inferred, or  
16 facilitated through dark patterns shall not constitute consent for any purpose.

17 (b) Individual Autonomy.—A covered entity may not condition, effectively condition, attempt  
18 to condition, or attempt to effectively condition the exercise of a right described in this Act  
19 through the use of any false, fictitious, fraudulent, or materially misleading statement or  
20 representation.

## 21 SEC. 8. PROHIBITION ON DENIAL OF SERVICE AND 22 WAIVER OF RIGHTS.

23 (a) Retaliation Through Service or Pricing Prohibited.—A covered entity may not retaliate  
24 against an individual for exercising any of the rights guaranteed by the Act, or any regulations  
25 promulgated under this Act, including denying products or services, charging different prices or  
26 rates for products or services, or providing a different level of quality of products or services.

27 (b) Rules of Construction.—

28 (1) BONA FIDE LOYALTY PROGRAMS.—

29 (A) IN GENERAL.—Nothing in subsection (a) may be construed to prohibit a covered  
30 entity from offering—

31 (i) a different price, rate, level, quality, or selection of products or services to an  
32 individual, including offering products or services for no fee, if the offering is in  
33 connection with an individual’s voluntary participation in a bona fide loyalty  
34 program, provided that—

35 (I) the individual provided affirmative express consent to participate in  
36 such bona fide loyalty program;

37 (II) the covered entity provides an individual with means to withdraw the

1 affirmative express consent previously provided by the individual in the  
2 manner set forth in section 3(b)(2);

3 (III) the covered entity abides by an individual’s exercise of any right  
4 described in sections 3(b)(2), 5, or 6; and

5 (IV) the individual provides affirmative express consent for the transfer of  
6 any data collected in connection with a bona fide loyalty program; and

7 (ii) different prices or functionalities with respect to a product or service based  
8 on an individual’s decision to terminate membership in a bona fide loyalty  
9 program or to exercise a right under section 5(a)(3) that deletes covered data that  
10 is strictly necessary for participation in the bona fide loyalty program.

11 (B) BONA FIDE LOYALTY PROGRAM DEFINED.—For purposes of this paragraph, the  
12 term “bona fide loyalty program” includes rewards, premium features, discounts, or  
13 club card programs offered by a covered entity that is not a covered high-impact social  
14 media company or data broker.

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

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

## 22 SEC. 9. DATA SECURITY AND PROTECTION OF 23 COVERED DATA.

24 (a) Establishment of Data Security Practices.—

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

27 (A) the confidentiality, integrity, and accessibility of covered data; and

28 (B) covered data against unauthorized access.

29 (2) CONSIDERATIONS.—The data security practices required under paragraph (1) shall be  
30 appropriate to—

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

32 (B) the nature and scope of the covered entity’s or the service provider’s collecting,  
33 processing, retaining, or transferring of covered data, taking into account such covered  
34 entity’s or service provider’s changing business operations with respect to covered  
35 data;

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

37 (D) the state-of-the-art (and limitations thereof) in administrative, technical, and  
38 physical safeguards for protecting such covered data.

1 (b) Specific Requirements.—The data security practices required under subsection (a) shall  
2 include, for each respective entity’s own system, at a minimum, the following practices:

3 (1) ASSESS VULNERABILITIES.—Routinely identifying and assessing any reasonably  
4 foreseeable internal or external risk to, and vulnerability in, each system maintained by the  
5 covered entity or service provider that collects, processes, retains, or transfers covered data,  
6 including unauthorized access to or corruption of such covered data, human vulnerabilities,  
7 access rights, and the use of service providers. Such activities shall include a plan to receive  
8 and consider unsolicited reports of vulnerability by any entity or individual, and, if such  
9 report is reasonably credible, perform a reasonable and timely investigation of such report  
10 and take appropriate action necessary to protect covered data against such vulnerability.

11 (2) PREVENTATIVE AND CORRECTIVE ACTION.—

12 (A) IN GENERAL.—Taking preventative and corrective action to mitigate any  
13 reasonably foreseeable internal or external risk or vulnerability to covered data  
14 identified by the covered entity or service provider, consistent with the nature of such  
15 risk or vulnerability and the covered entity’s or service provider’s role in collecting,  
16 processing, retaining, or transferring the data, which may include implementing  
17 administrative, technical, or physical safeguards or changes to data security practices  
18 or the architecture, installation, or implementation of network or operating software.

19 (B) EVALUATION OF PREVENTATIVE AND CORRECTIVE ACTION.—Evaluating and  
20 making reasonable adjustments to the action described in subparagraph (A) in light of  
21 any material changes in technology, internal or external threats to covered data, and the  
22 covered entity’s or service provider’s changing business operations with respect to  
23 covered data.

24 (3) INFORMATION RETENTION AND DISPOSAL.—Disposing of covered data (either by or at  
25 the direction of a covered entity) that is required to be deleted by law or is no longer  
26 necessary for the purpose for which the data was collected, processed, retained, or  
27 transferred, unless an individual has provided affirmative express consent to such retention.  
28 Such disposal shall include destroying, permanently erasing, or otherwise modifying the  
29 covered data to make such data permanently unreadable or indecipherable and  
30 unrecoverable to ensure ongoing compliance with this section.

31 (4) RETENTION SCHEDULE.—Developing, maintaining, and adhering to a retention  
32 schedule for covered data disposal consistent with the practices and procedures required in  
33 paragraph (3).

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

36 (6) INCIDENT RESPONSE.—Implementing procedures to detect, respond to, and recover  
37 from data security incidents, including breaches of data security.

38 (c) Regulations.—The Commission may, in consultation with the Secretary of Commerce,  
39 promulgate in accordance with section 553 of title 5, United States Code, technology-neutral,  
40 process-based regulations to carry out this section.

## 41 SEC. 10. EXECUTIVE RESPONSIBILITY.

1 (a) Designation of Privacy and Data Security Officers.—

2 (1) DESIGNATION.—

3 (A) IN GENERAL.—Except for an entity that is a large data holder, a covered entity or  
4 service provider shall designate 1 or more qualified employees to serve as privacy or  
5 data security officers.

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

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

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

13 (2) REQUIREMENTS FOR LARGE DATA HOLDERS.—

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

17 (B) ANNUAL CERTIFICATION.—

18 (i) IN GENERAL.—Beginning 1 year after the date of enactment of this Act, the  
19 chief executive officer of a large data holder (or, if the large data holder does not  
20 have a chief executive officer, the highest ranking officer of the large data holder)  
21 and each privacy officer and data security officer of such large data holder  
22 designated under subparagraph (A) shall annually certify to the Commission, in a  
23 manner specified by the Commission, that the large data holder maintains—

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

25 (II) internal reporting structures (as described in subparagraph (C)) to  
26 ensure that such certifying officers are involved in, and responsible for,  
27 decisions that impact compliance by the large data holder with this Act.

28 (ii) REQUIREMENTS.—A certification submitted under clause (i) shall be based  
29 on a review of the effectiveness of a large data holder's internal controls and  
30 reporting structures that is conducted by the certifying officers not more than 90  
31 days before the submission of the certification.

32 (C) INTERNAL REPORTING STRUCTURE REQUIREMENTS.—At least 1 of the officers  
33 described in subparagraph (A) shall, either directly or through a supervised designee—

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

36 (ii) conduct biennial and comprehensive audits to ensure the policies, practices,  
37 and procedures of the large data holder comply with this Act and, upon request,  
38 make such audits available to the Commission;

39 (iii) develop a program to educate and train employees about the requirements  
40 of this Act;

- (iv) maintain updated, accurate, clear, and understandable records of all material privacy and data security practices of the large data holder; and
- (v) serve as the point of contact between the large data holder and enforcement authorities.

(D) PRIVACY IMPACT ASSESSMENTS.—

(i) IN GENERAL.—Not later than 1 year after the date of enactment of this Act or 1 year after the date that an entity first meets the definition of large data holder, whichever is earlier, and biennially thereafter, each large data holder shall conduct a privacy impact assessment that weighs the benefits of the entity’s covered data collection, processing, retention, and transfer practices against the potential adverse consequences of such practices to individual privacy.

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

(I) reasonable and appropriate in scope given—

(aa) the nature and volume of the covered data collected, processed, retained, or transferred by the large data holder; and

(bb) the potential risks posed to the privacy of individuals by the collection, processing, retention, and transfer of covered data by the large data holder;

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

(III) approved by the privacy officer of the large data holder.

(iii) ADDITIONAL FACTORS TO INCLUDE IN ASSESSMENT.—In assessing the privacy risks, the large data holder shall include reviews of the means by which emerging technologies, including blockchain, distributed ledger technologies, privacy enhancing technologies, and other emerging technologies are used to secure covered data.

## SEC. 11. SERVICE PROVIDERS AND THIRD PARTIES.

(a) Service Providers.—

(1) IN GENERAL.—A service provider—

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

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

(C) shall assist a covered entity in fulfilling the covered entity’s obligations to respond to consumer rights requests pursuant to sections 5, 6, and 14 by appropriate

1 technical and organizational measures, taking into account the nature of the processing  
2 and the information reasonably available to the service provider;

3 (D) shall, upon the reasonable request of the covered entity, make available to the  
4 covered entity information necessary to demonstrate the service provider’s compliance  
5 with the requirements of this Act;

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

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

15 (G) shall develop, implement, and maintain reasonable administrative, technical, and  
16 physical safeguards that are designed to protect the security and confidentiality of  
17 covered data the service provider processes consistent with section 9; and

18 (H) shall—

19 (i) allow and cooperate with reasonable assessments by the covered entity; or

20 (ii) arrange for a qualified and independent assessor to conduct an assessment  
21 of the service provider’s policies and technical and organizational measures in  
22 support of the obligations under this Act, using an appropriate and accepted  
23 control standard or framework and assessment procedure for such assessments  
24 and report the results of such assessment to the covered entity.

25 (2) CONTRACT REQUIREMENTS.—A contract between a covered entity and a service  
26 provider—

27 (A) shall govern the service provider’s data processing procedures with respect to  
28 any collection, processing, retention, or transfer performed on behalf of the covered  
29 entity;

30 (B) shall clearly set forth—

31 (i) instructions for collecting, processing, retaining, or transferring data;

32 (ii) the nature and purpose of the collection, processing, retention, or transfer;

33 (iii) the type of data subject to collection, processing, retention, or transfer;

34 (iv) the duration of the processing or retention; and

35 (v) the rights and obligations of both parties;

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

38 (D) shall prohibit—

39 (i) the collection, processing, retention, or transfer of covered data in a manner

1 that does not comply with the requirements of paragraph (1); and

2 (ii) combining service provider data with covered data which the service  
3 provider receives from or on behalf of another entity or collects from the  
4 interaction of the service provider with an individual, provided that such  
5 combining is not necessary to effectuate a purpose described in section 3(d) and is  
6 otherwise permitted under the contract required by this subsection.

7 (b) Third Parties.—A third party—

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

9 (A) in the case of sensitive covered data, the purpose for which an individual gave  
10 affirmative express consent for the transfer of the individual’s sensitive covered data;  
11 or

12 (B) in the case of covered data that is not sensitive covered data, a purpose for which  
13 the covered entity or service provider made a disclosure pursuant to section 4;

14 (2) for purposes of paragraph (1), may reasonably rely on representations made by the  
15 covered entity that transferred the third-party data regarding the expectations of a  
16 reasonable person based on disclosures by the covered entity about the treatment of such  
17 data, provided that the third party conducts reasonable due diligence on the representations  
18 of the covered entity and finds those representations to be credible; and

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

22 (c) Rules of Construction.—

23 (1) SUCCESSIVE ACTOR VIOLATIONS.—

24 (A) IN GENERAL.—With respect to a violation of this Act by a service provider or  
25 third party regarding covered data received by the service provider or third party from  
26 a covered entity, the covered entity that transferred such covered data to the service  
27 provider or third party shall not be in violation of this Act if the covered entity  
28 transferred the covered data to the service provider or third party in compliance with  
29 the requirements of this Act and, at the time of transferring such covered data, the  
30 entity did not have actual knowledge, or reason to believe, that the service provider or  
31 third party intended to violate this Act.

32 (B) KNOWLEDGE OF VIOLATION.—An entity that transfers covered data to a service  
33 provider or third party and has actual knowledge, or reason to believe, that such service  
34 provider or third party is violating, or is about to violate, the requirements of this Act  
35 shall immediately cease the transfer of covered data to such service provider or third  
36 party.

37 (2) PRIOR ACTOR VIOLATIONS.—An entity that collects, processes, retains, or transfers  
38 covered data in compliance with the requirements of this Act shall not be in violation of this  
39 Act as a result of a violation by an entity from which it receives, or on whose behalf it  
40 collects, processes, retains, or transfers, covered data.

41 (d) Due Diligence.—

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

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

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

## 7 SEC. 12. DATA BROKERS.

8 (a) Notice.—A data broker shall—

9 (1) establish and maintain a publicly accessible website; and

10 (2) place a clear, conspicuous, not misleading, and readily accessible notice on the  
11 publicly accessible website and any mobile application of the data broker that—

12 (A) the entity is a data broker, using specific language that the Commission shall  
13 develop through guidance not later than 180 days after the date of enactment of this  
14 Act;

15 (B) an individual has a right to exercise the rights described in sections 5 and 6,  
16 including a link or other tool to allow an individual to exercise such rights;

17 (C) includes a link to the website established under subsection (c)(3); and

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

19 (b) Prohibited Practices.—A data broker is prohibited from—

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

22 (A) stalking or harassing another individual; or

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

24 (2) misrepresenting the business practices of the data broker.

25 (c) Data Broker Registration.—

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

30 (2) REGISTRATION REQUIREMENTS.—In registering with the Commission as required  
31 under paragraph (1), a data broker shall do the following:

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

33 (B) Provide the Commission with the following information:

34 (i) The legal name and primary physical, email, and internet addresses of the  
35 data broker.

36 (ii) A description of the categories of covered data the data broker collects,



1 processes, retains, and transfers.

2 (iii) The contact information of the data broker, including the name of a contact  
3 person, a monitored telephone number, a monitored e-mail address, a website, and  
4 a physical mailing address.

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

7 (3) DATA BROKER REGISTRY.—

8 (A) ESTABLISHMENT.—The Commission shall establish and maintain on a publicly  
9 available website a searchable registry of data brokers that are registered with the  
10 Commission under this subsection.

11 (B) REQUIREMENTS.—The registry established under subparagraph (A) shall—

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

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

15 (iii) includes a mechanism by which an individual may submit a request to all  
16 registered data brokers that are not consumer reporting agencies (as defined in  
17 section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f))), and to the  
18 extent such third-party collecting entities are not acting as consumer reporting  
19 agencies (as so defined), a “Do Not Collect” directive such that any registered  
20 data broker shall ensure that the data broker no longer collects covered data  
21 related to such individual without the affirmative express consent of such  
22 individual, except insofar as the data broker is acting as a service provider.

23 (4) DO NOT COLLECT REQUESTS.—

24 (A) COMPLIANCE.—Subject to subparagraph (B), each data broker that receives a  
25 request from an individual using the mechanism established under paragraph (3)(B)(iii)  
26 shall comply with such request not later than 30 days after receiving such request.

27 (B) EXCEPTION.—A data broker may decline to fulfill a request from an individual  
28 where—

29 (i) the data broker has actual knowledge that the individual has been convicted  
30 of a crime related to the abduction or sexual exploitation of a child; and

31 (ii) the data collected by the data broker is necessary—

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

33 (II) for the Congressionally designated entity that serves as the nonprofit  
34 national resource center and clearinghouse to provide assistance to victims,  
35 families, child-serving professionals, and the general public regarding issues  
36 related to missing and exploited children.

37 (d) Penalties.—

38 (1) IN GENERAL.—Subject to paragraph (2), a data broker that violates this section shall  
39 be liable for civil penalties as set forth in subsections (l) and (m) of section 5 of the Federal

1 Trade Commission Act, (15 U.S.C. 45(l), (m)).

2 (2) EXCEPTIONS.—A data broker that—

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

5 (i) a civil penalty of \$100 for each day the data broker fails to register, not to  
6 exceed a total of \$10,000 for any year; and

7 (ii) an amount equal to the registration fee due under subsection (c)(2)(A) for  
8 each year that the data broker failed to register as required under subsection  
9 (c)(1); or

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

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

## 16 SEC. 13. CIVIL RIGHTS AND ALGORITHMS.

17 (a) Civil Rights Protections.—

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

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

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

25 (i) a covered entity's or a service provider's self-testing to prevent or mitigate  
26 unlawful discrimination; or

27 (ii) diversifying an applicant, participant, or customer pool;

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

30 (C) advertising, marketing, or soliciting economic opportunities or benefits to  
31 underrepresented populations or members of protected classes as described in  
32 paragraph (1).

33 (b) FTC Enforcement Assistance.—

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

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

4 (A) the types of information the Commission transmitted to Executive agencies  
5 under paragraph (1) during the previous 1-year period; and

6 (B) how such information relates to Federal civil rights laws.

7 (3) TECHNICAL ASSISTANCE.—In transmitting information under paragraph (1), the  
8 Commission may consult and coordinate with, and provide technical and investigative  
9 assistance, as appropriate, to such Executive agency.

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

13 (c) Covered Algorithm Impact and Evaluation.—

14 (1) COVERED ALGORITHM IMPACT ASSESSMENT.—

15 (A) IMPACT ASSESSMENT.—Notwithstanding any other provision of law, not later  
16 than 2 years after the date of enactment of this Act, and annually thereafter, a large  
17 data holder that uses a covered algorithm in a manner that poses a consequential risk of  
18 a harm identified under subparagraph (B)(vi) to an individual or group of individuals  
19 and uses such covered algorithm, solely or in part, to collect, process, or transfer  
20 covered data shall conduct an impact assessment of such algorithm in accordance with  
21 subparagraph (B).

22 (B) IMPACT ASSESSMENT SCOPE.—The impact assessment required under  
23 subparagraph (A) shall provide the following:

24 (i) A detailed description of the design process and methodologies of the  
25 covered algorithm.

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

27 (iii) A detailed description of the data used by the covered algorithm, including  
28 the specific categories of data that will be processed as input and any data used to  
29 train the model that the covered algorithm relies on, if applicable.

30 (iv) A description of the outputs produced by the covered algorithm.

31 (v) An assessment of the necessity and proportionality of the covered algorithm  
32 in relation to its stated purpose.

33 (vi) A detailed description of steps the large data holder has taken or will take  
34 to mitigate potential harms from the covered algorithm to an individual or group  
35 of individuals, including related to—

36 (I) covered minors;

37 (II) making or facilitating advertising for, or determining access to, or  
38 restrictions on the use of housing, education, employment, healthcare,  
39 insurance, or credit opportunities;

1 (III) determining access to, or restrictions on the use of, any place of  
2 public accommodation, particularly as such harms relate to the protected  
3 characteristics of individuals, including race, color, religion, national origin,  
4 sex, or disability;

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

7 (V) disparate impact on the basis of individuals' political party registration  
8 status.

9 (2) ALGORITHM DESIGN EVALUATION.—Notwithstanding any other provision of law, not  
10 later than 2 years after the date of enactment of this Act, a covered entity or service provider  
11 that knowingly develops a covered algorithm shall, prior to deploying the covered algorithm  
12 in interstate commerce, evaluate the design, structure, and inputs of the covered algorithm,  
13 including any training data used to develop the covered algorithm, to reduce the risk of the  
14 potential harms identified under paragraph (1)(B)(vi).

15 (3) OTHER CONSIDERATIONS.—

16 (A) FOCUS.—In complying with paragraphs (1) and (2), a covered entity and a  
17 service provider may focus the impact assessment or evaluation on any covered  
18 algorithm, or portions of a covered algorithm, that will be put to use and may  
19 reasonably contribute to the risk of the potential harms identified under paragraph  
20 (1)(B)(vi).

21 (B) AVAILABILITY.—

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

23 (I) shall, not later than 30 days after completing an impact assessment or  
24 evaluation under paragraph (1) or (2), submit the impact assessment or  
25 evaluation to the Commission;

26 (II) shall, upon request, make such impact assessment and evaluation  
27 available to Congress; and

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

30 (ii) TRADE SECRETS.—A covered entity or service provider may redact and  
31 segregate any trade secret (as defined in section 1839 of title 18, United States  
32 Code) or other confidential or proprietary information from public disclosure  
33 under this subparagraph, and the Commission shall abide by its obligations under  
34 section 6(f) of the Federal Trade Commission Act (15 U.S.C. 46(f)) with respect  
35 to such information.

36 (C) LIMITATION ON ENFORCEMENT.—

37 (i) IN GENERAL.—Subject to clause (ii), the Commission may not use any  
38 information obtained solely and exclusively through a covered entity or a service  
39 provider's disclosure of information to the Commission in compliance with this  
40 section for any purpose other than to carry out the provisions of this Act,  
41 including the study and report described in paragraph (6).

1 (ii) EXCEPTIONS.—

2 (I) PROVISION TO CONGRESS.—The limitation described in clause (i) does  
3 not preclude the Commission from providing such information to Congress  
4 in response to a subpoena.

5 (II) CONSENT ORDERS.—The limitation described in clause (i) does not  
6 preclude the Commission from enforcing a consent order entered into with  
7 the applicable covered entity or service provider.

8 (4) GUIDANCE.—Not later than 2 years after the date of enactment of this Act, the  
9 Commission shall, in consultation with the Secretary of Commerce, publish guidance  
10 regarding compliance with this section.

11 (5) RULEMAKING AND EXEMPTION.—The Commission may promulgate regulations, in  
12 accordance with section 553 of title 5, United States Code, as necessary to establish  
13 processes by which a—

14 (A) large data holder shall submit an impact assessment to the Commission under  
15 paragraph (3)(B)(i)(I); and

16 (B) large data holder, covered entity, or service provider may exclude from this  
17 subsection any covered algorithm that presents low or minimal risk of the potential  
18 harms identified under paragraph (1)(B)(vi) to an individual or group of individuals.

19 (6) STUDY AND REPORT.—

20 (A) STUDY.—The Commission, in consultation with the Secretary of Commerce,  
21 shall conduct a study, to review any impact assessment or evaluation submitted under  
22 this subsection. Such study shall include an examination of—

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

24 (ii) methods to reduce the risk of harm to individuals that may be related to the  
25 use of covered algorithms.

26 (B) REPORT.—

27 (i) INITIAL REPORT.—Not later than 3 years after the date of enactment of this  
28 Act, the Commission, in consultation with the Secretary of Commerce, shall  
29 submit to Congress a report containing the results of the study conducted under  
30 subparagraph (A), together with recommendations for such legislation and  
31 administrative action as the Commission determines appropriate.

32 (ii) ADDITIONAL REPORTS.—Not later than 3 years after submission of the  
33 initial report under clause (i), and as the Commission determines necessary  
34 thereafter, the Commission shall submit to Congress an updated version of such  
35 report.

## 36 SEC. 14. CONSEQUENTIAL DECISION OPT OUT.

37 (a) In General.—An entity that uses a covered algorithm to make or facilitate a consequential  
38 decision shall—

39 (1) provide—

- 1 (A) notice to any individual subject to such use of the covered algorithm; and
- 2 (B) an opportunity for the individual to opt out of such use of the covered algorithm;
- 3 and

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

5 (b) Notice.—The notice required under subsection (a)(1)(A) shall—

- 6 (1) be clear, conspicuous, and not misleading;
- 7 (2) provide meaningful information about how the covered algorithm makes or facilitates
- 8 a consequential decision, including the range of potential outcomes;

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

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

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

12 (4) be reasonably accessible to and usable by individuals with disabilities.

13 (c) Guidance.—Not later than 2 years after the date of enactment of this Act, the Commission,  
14 in consultation with the Secretary of Commerce, shall publish guidance regarding compliance  
15 with this section.

16 (d) Consequential Decision Defined.—For the purposes of this section, the term  
17 “consequential decision” means a determination or an offer, including through advertisement,  
18 that uses covered data and relates to—

19 (1) an individual’s or a class of individuals’ access to or equal enjoyment of housing,  
20 employment, education enrollment or opportunity, healthcare, insurance, or credit  
21 opportunities; or

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

## 23 SEC. 15. COMMISSION APPROVED COMPLIANCE 24 GUIDELINES.

25 (a) Application for Compliance Guideline Approval.—

26 (1) IN GENERAL.—A covered entity that is not a data broker and is not a large data holder,  
27 may apply to the Commission for approval of 1 or more sets of compliance guidelines  
28 governing the collection, processing, retention, and transfer of covered data by the covered  
29 entity.

30 (2) APPLICATION REQUIREMENTS.—Such application shall include—

31 (A) a description of how the proposed compliance guidelines will meet or exceed  
32 the requirements of this Act;

33 (B) a description of the entities or activities the proposed set of compliance  
34 guidelines is designed to cover;

35 (C) a list of the covered entities, to the extent known at the time of application, that  
36 intend to adhere to the compliance guidelines;

1 (D) a description of the independent organization, which shall not be associated with  
2 any of the participating covered entities, that will administer the compliance  
3 guidelines; and

4 (E) and a description of how such entities will be assessed for adherence to such  
5 compliance guidelines by the independent organization described in subparagraph (D).

6 (3) COMMISSION REVIEW.—

7 (A) INITIAL APPROVAL.—

8 (i) PUBLIC COMMENT PERIOD.—Not later than 90 days after receiving an  
9 application under paragraph (1), the Commission shall publish the application and  
10 provide an opportunity for public comment on the compliance guidelines  
11 proposed in such application.

12 (ii) APPROVAL CRITERIA.—The Commission shall approve an application  
13 submitted under paragraph (1), including the independent organization the  
14 application proposed to administer the compliance guidelines proposed in such  
15 application, if the applicant demonstrates that the compliance guidelines—

16 (I) meet or exceed requirements of this Act;

17 (II) will provide for the regular review and validation by the independent  
18 organization to ensure that the covered entity continues to meet or exceed the  
19 requirements of this Act; and

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

25 (iii) TIMELINE.—Not later than 1 year after receiving an application under  
26 paragraph (1), the Commission shall issue a determination approving or denying  
27 the application, including the independent organization the application proposed  
28 to administer the compliance guidelines proposed in such application, and  
29 providing an explanation for such approval or denial.

30 (B) APPROVAL OF MODIFICATIONS.—

31 (i) IN GENERAL.—If the independent organization administering a set of  
32 compliance guidelines makes any material change to guidelines previously  
33 approved by the Commission, the independent organization shall submit the  
34 updated compliance guidelines to the Commission for approval. As soon as  
35 feasible, the Commission shall publish the updated compliance guidelines and  
36 provide an opportunity for public comment.

37 (ii) TIMELINE.—Not later than 1 year after receiving the updated compliance  
38 guidelines under clause (i), the Commission shall issue a determination approving  
39 or denying the material change to such guidelines.

40 (b) Withdrawal of Approval.—

1 (1) IN GENERAL.—If at any time the Commission determines that compliance guidelines  
2 previously approved under this section no longer meet the requirements of this Act or a  
3 regulation promulgated under this Act, or that compliance with any such approved  
4 guidelines is insufficiently enforced by the independent organization administering the  
5 guidelines, the Commission shall notify the relevant covered entity and independent  
6 organization of the Commission’s determination to withdraw approval of such guidelines,  
7 including the basis for such determination.

8 (2) OPPORTUNITY TO CURE.—

9 (A) IN GENERAL.—Not later than 180 days after receiving notice from the  
10 Commission under paragraph (1), a covered entity and independent organization may  
11 cure any alleged deficiency with the compliance guidelines or the enforcement thereof  
12 and submit each proposed cure to the Commission.

13 (B) EFFECT ON WITHDRAWAL OF APPROVAL.—If the Commission determines that the  
14 proposed cures described in subparagraph (A) eliminate the alleged deficiency in the  
15 compliance guidelines, then the Commission may not withdraw approval of such  
16 guidelines on the basis of such determination.

17 (c) Certification.—A covered entity with compliance guidelines approved by the Commission  
18 under this section shall—

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

21 (2) as part of such self-certification, indicate the independent organization responsible for  
22 assessing compliance with such compliance guidelines.

23 (d) Rebuttable Presumption of Compliance.—A covered entity with compliance guidelines  
24 approved by the Commission under this section, and that is in compliance with such guidelines,  
25 shall be entitled to a rebuttable presumption that such entity is in compliance with the relevant  
26 provisions of this Act if such covered entity is in compliance with such guidelines.

## 27 SEC. 16. PRIVACY-ENHANCING TECHNOLOGY PILOT 28 PROGRAM.

29 (a) In General.—Not later than 1 year after the date of enactment of this Act, the Commission  
30 shall establish and carry out a pilot program to encourage private sector use of privacy-enhancing  
31 technology for the purpose of protecting covered data in compliance with section 9.

32 (b) Covered Entity Participation.—

33 (1) APPLICATION PROCESS.—A covered entity seeking to participate in the pilot program  
34 established under subsection (a) shall submit to the Commission, in such time, form, and  
35 manner as the Commission may require, an application that demonstrates the ability of the  
36 covered entity to use privacy-enhancing technology to establish data security practices that  
37 meet or exceed the requirements of section 9.

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

40 (A) with respect to any action under section 17 or 18 for a violation of section 9, be



1 deemed to be in compliance with section 9 with respect to any covered data subject to  
2 the privacy-enhancing technology; and

3 (B) for any action under section 19 alleging a data breach due to a violation of  
4 section 9, be entitled to a rebuttable presumption that such covered entity is in  
5 compliance with the relevant requirements under section 9 with respect to any covered  
6 data subject to the privacy-enhancing technology.

7 (3) AUDIT OF COVERED ENTITIES.—

8 (A) IN GENERAL.—The Commission shall, on an ongoing basis, audit each covered  
9 entity participating in the pilot program to determine whether the covered entity is  
10 maintaining the use and implementation of privacy-enhancing technology to secure  
11 covered data.

12 (B) REMOVAL.—

13 (i) IN GENERAL.—If at any time the Commission determines that a covered  
14 entity participating in the pilot program is no longer maintaining the use and  
15 implementation of privacy-enhancing technology, the Commission shall—

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

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

20 (ii) OPPORTUNITY TO CURE.—Not later than 180 days after receiving notice  
21 from the Commission under clause (i), a covered entity may cure any alleged  
22 deficiency with its use and implementation of privacy-enhancing technology and  
23 submit to the Commission such proposed cure. If the Commission determines that  
24 such cure eliminates the alleged deficiency, then the Commission may not remove  
25 the covered entity from participation in the pilot program.

26 (c) Coordination.—In carrying out the pilot program under subsection (a), the Commission  
27 shall—

28 (1) solicit input from private, public, and academic stakeholders; and

29 (2) in consultation with the Secretary of Commerce, develop ongoing public and private  
30 sector engagement to disseminate voluntary, consensus-based resources to increase the  
31 integration of privacy-enhancing technology in data collection, sharing, and analytics by the  
32 public and private sectors.

33 (d) GAO Study and Report.—

34 (1) STUDY.—Not later than 3 years after the date of enactment of this Act, the  
35 Comptroller General of the United States (in this subsection referred to as the “Comptroller  
36 General”) shall conduct a study to—

37 (A) assess the progress of the pilot program established under subsection (a);

38 (B) evaluate the Commission’s use of privacy-enhancing technology to support  
39 oversight of covered entities’ data security practices; and

40 (C) develop recommendations to improve and advance privacy-enhancing

1 technology, including by improving communication and coordination between covered  
2 entities and the Commission to increase use and implementation of privacy-enhancing  
3 technology by such entities and the Commission.

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

8 (3) FINAL REPORT.—Not later than 240 days after the initial briefing under paragraph (2),  
9 the Comptroller General shall submit to the Committee on Commerce, Science, and  
10 Transportation of the Senate and the Committee on Energy and Commerce of the House of  
11 Representatives a final report describing the results of the study conducted under paragraph  
12 (1), including the recommendations developed under subparagraph (C) of such paragraph.

13 (e) Sunset.—The Commission shall terminate the pilot program established under subsection  
14 (a) not later than 10 years after the date on which the pilot program is established.

15 (f) Privacy-enhancing Technology Defined.—The term “privacy-enhancing technology”—

16 (1) means any software or hardware solution, cryptographic algorithm, or other technical  
17 process of extracting the value of the information without risking the privacy and security of  
18 the information; and

19 (2) includes other technologies with functionality similar to homomorphic encryption,  
20 differential privacy, zero-knowledge proofs, synthetic data generation, federated learning,  
21 and secure multi-party computation.

## 22 SEC. 17. ENFORCEMENT BY THE FEDERAL TRADE 23 COMMISSION.

24 (a) New Bureau.—

25 (1) IN GENERAL.—The Commission shall establish within the Commission a new bureau  
26 comparable in structure, size, organization, and authority to the existing bureaus within the  
27 Commission related to consumer protection and competition.

28 (2) MISSION.—The mission of the bureau established under this subsection shall be to  
29 assist the Commission in exercising the Commission’s authority under this Act and related  
30 authorities.

31 (3) TIMELINE.—The bureau shall be established, staffed, and fully operational not later  
32 than 1 year after the date of enactment of this Act.

33 (b) Enforcement by the Federal Trade Commission.—

34 (1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act, or a regulation  
35 promulgated under this Act, shall be treated as a violation of a rule defining an unfair or  
36 deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade  
37 Commission Act (15 U.S.C. 57a(a)(1)(B)).

38 (2) POWERS OF THE COMMISSION.—

39 (A) IN GENERAL.—Except as provided in paragraphs (3) and (4) or otherwise

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

6 (B) PRIVILEGES AND IMMUNITIES.—Any entity that violates this Act or a regulation  
7 promulgated under this Act shall be subject to the penalties and entitled to the  
8 privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C.  
9 41 et seq.).

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

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

17 (B) organizations not organized to carry on business for their own profit or that of  
18 their members.

19 (4) PRIVACY AND SECURITY VICTIMS RELIEF FUND.—

20 (A) ESTABLISHMENT.—There is established in the Treasury of the United States a  
21 separate fund to be known as the “Privacy and Security Victims Relief Fund” (referred  
22 to in this paragraph as the “Victims Relief Fund”).

23 (B) DEPOSITS.—

24 (i) DEPOSITS FROM THE COMMISSION.—The Commission shall deposit into the  
25 Victims Relief Fund the amount of any civil penalty obtained against any entity in  
26 any judicial or administrative action the Commission commences to enforce this  
27 Act or a regulation promulgated under this Act.

28 (ii) DEPOSITS FROM THE ATTORNEY GENERAL OF THE UNITED STATES.—The  
29 Attorney General of the United States shall deposit into the Victims Relief Fund  
30 the amount of any civil penalty obtained against any entity in any judicial or  
31 administrative action the Attorney General commences on behalf of the  
32 Commission to enforce this Act or a regulation promulgated under this Act.

33 (C) USE OF FUND AMOUNTS.—

34 (i) AVAILABILITY TO THE COMMISSION.—Notwithstanding section 3302 of title  
35 31, United States Code, amounts in the Victims Relief Fund shall be available to  
36 the Commission, without fiscal year limitation, to provide redress, payments or  
37 compensation, or other monetary relief to persons affected by an act or practice  
38 for which civil penalties have been obtained under this Act.

39 (ii) OTHER PERMISSIBLE USES.—To the extent that individuals cannot be located  
40 or such redress, payments or compensation, or other monetary relief are otherwise  
41 not practicable, the Commission may use such funds for the purpose of—

1 (I) consumer or business education relating to privacy and data security; or

2 (II) engaging in technological research that the Commission considers  
3 necessary to enforce this Act.

4 (D) CALCULATION.—

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

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

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

18 (c) Report.—

19 (1) IN GENERAL.—Not later than 4 years after the date of the enactment of this Act, and  
20 annually thereafter, the Commission shall, submit to Congress a report on investigations  
21 conducted for alleged violations this Act, including—

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

23 (B) the number of such investigations the Commission has closed with no official  
24 agency action;

25 (C) the disposition of such investigations, if such investigations have concluded and  
26 resulted in official agency action; and

27 (D) for each investigation that was closed with no official agency action the industry  
28 sectors of the covered entities subject to each investigation.

29 (2) PRIVACY PROTECTIONS.—The report required under paragraph (1) shall not include  
30 the identity of the person who is the subject of the investigation or any other information  
31 that identifies such person.

32 (3) ANNUAL PLAN.—Not later than 540 days after the date of the enactment of this Act,  
33 and annually thereafter, the Commission shall submit to Congress a plan for the next  
34 calendar year describing the projected activities of the Commission under this Act,  
35 including each of the following:

36 (A) The policy priorities of the Commission and any changes to the previous policy  
37 priorities of the Commission.

38 (B) Any rulemaking proceedings projected to be commenced, including any such  
39 proceedings to amend or repeal a rule.

40 (C) Any plans to develop, update, or withdraw guidance required under this Act.

1 (D) Any plans to restructure the Commission or establish, alter, or terminate  
2 working groups.

3 (E) Projected dates and timelines, or changes to projected dates and timelines,  
4 associated with any of the requirements under this Act.

## 5 SEC. 18. ENFORCEMENT BY STATES.

### 6 (a) Civil Action.—

7 (1) IN GENERAL.—In any case in which the attorney general of a State, the chief  
8 consumer protection officer of a State, or an officer or office of the State authorized to  
9 enforce privacy or data security laws applicable to covered entities or service providers has  
10 reason to believe that an interest of the residents of that State has been or is adversely  
11 affected by the engagement of any entity in an act or practice that violates this Act or a  
12 regulation promulgated under this Act, the attorney general, chief consumer protection  
13 officer, or other authorized officer of the State may bring a civil action in the name of the  
14 State, or as parens patriae on behalf of the residents of the State, in an appropriate Federal  
15 district court of the United States to—

16 (A) enjoin that act or practice;

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

18 (C) obtain civil penalties;

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

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

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

24 (2) LIMITATION.—In any case where the attorney general of a State, the chief consumer  
25 protection officer of a State, or an officer or office of the State authorized to enforce privacy  
26 or data security laws applicable to covered entities or service providers brings an action  
27 under paragraph (1), no other officer of the same State may institute a civil action under  
28 paragraph (1) against the same defendant for the same violation of this Act or a regulation  
29 promulgated under this Act.

### 30 (b) Rights of the Commission.—

31 (1) IN GENERAL.—Except where not feasible, the State officer shall notify the  
32 Commission in writing prior to initiating a civil action under subsection (a). Such notice  
33 shall include a copy of the complaint to be filed to initiate such action. Upon receiving such  
34 notice, the Commission may intervene in such action and, upon intervening—

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

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

37 (2) NOTIFICATION TIMELINE.—Where it is not feasible for the State officer to provide the  
38 notification required by paragraph (1) before initiating a civil action under subsection (a),  
39 the State officer shall notify the Commission immediately after initiating the civil action.

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

8 (d) Investigatory Powers.—Nothing in this section shall be construed to prevent the attorney  
9 general of a State, the chief consumer protection officer of a State, or an officer or office of a  
10 State authorized to enforce privacy or data security laws applicable to covered entities or service  
11 providers from exercising the powers conferred on such officer or office to conduct  
12 investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or  
13 the production of documentary or other evidence.

14 (e) Venue; Service of Process.—

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

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

20 (A) is an inhabitant; or

21 (B) may be found.

22 (f) GAO Study.—Not later than 1 year after the date of enactment of this Act, the Comptroller  
23 General of the United States shall conduct a study on State attorneys general’s hiring of, or  
24 otherwise contracting with, outside firms to assist in the enforcement of this Act. The study shall  
25 include—

26 (1) the frequency of such hires;

27 (2) the contingency fees or hourly rates and other costs of hiring or contracting with  
28 outside firms;

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

30 (4) the bid process for such outside law firm work and selection process, including  
31 reviews of conflicts of interest;

32 (5) the practices State attorneys general set in place to protect sensitive information that  
33 would become accessible by outside firms while they are assisting in enforcement efforts;

34 (6) the percent of monetary recovery that is returned to victims and the percent that is  
35 retained by the law firm; and

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

37 (g) Calculation.—Any amount that a court orders an entity to pay in an action brought under  
38 subsection (a) shall be offset by any amount the person received from an action brought against  
39 the entity for the same violation under section 17 or 19.

40 (h) Preservation of State Powers.—Except as provided in subsection (c), no provision of this

1 section shall be construed as altering, limiting, or affecting the authority of a State attorney  
2 general, the chief consumer protection officer of a State, or an officer or office of a State  
3 authorized to enforce laws applicable to covered entities or service providers to—

4 (1) bring an action or other regulatory proceeding arising solely under the laws in effect  
5 in that State; or

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

## 10 SEC. 19. ENFORCEMENT BY INDIVIDUALS.

### 11 (a) Enforcement by Individuals.—

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

### 19 (2) RELIEF.—

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

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

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

25 (iii) declaratory relief; and

26 (iv) reasonable attorney’s fees and litigation costs.

27 (B) BIOMETRIC AND GENETIC INFORMATION.—In a civil action brought under  
28 paragraph (1) for a violation of this Act with respect to section 3(c) where the conduct  
29 underlying the violation occurred primarily and substantially in Illinois, in which the  
30 plaintiff prevails, the court may award the plaintiff—

31 (i) the same relief as set forth in section 20 of the Biometric Information  
32 Privacy Act (740 ILCS 14/20), as such statute read on January 1, 2024; or

33 (ii) the same relief as set forth in section 40 of the Genetic Information Privacy  
34 Act (740 ILCS 513/40), as such statute read on January 1, 2024.

### 35 (C) DATA SECURITY.—

36 (i) IN GENERAL.—In a civil action brought under paragraph (1) for a violation  
37 of section 9, alleging unauthorized access of covered information (as defined in  
38 clause (ii)) in which the plaintiff prevails, the court may award a plaintiff who is a  
39 resident of California the same relief as set forth in section 1798.150 of the

1 California Civil Code, as such statute read on January 1, 2024.

2 (ii) COVERED INFORMATION DEFINED.—For purposes of this subparagraph, the  
3 term “covered information” means—

4 (I) an individual’s username, email address, or telephone number in  
5 combination with a password or security question or answer that would  
6 permit access to an account held by the individual that contains or provides  
7 access to sensitive covered data; or

8 (II) an individual’s first name or first initial and the individual’s last name  
9 in combination with 1 or more of the following categories of sensitive  
10 covered data, when either the name or the sensitive covered data are not  
11 encrypted or redacted:

12 (aa) A government identifier as described in section 2(34)(A)(i).

13 (bb) Any sensitive covered data described in section 2(34)(A)(iv).

14 (cc) Health information, but only to the extent that such information  
15 reveals the individual’s history of medical treatment or diagnosis by a  
16 health care professional.

17 (dd) Biometric information.

18 (ee) Genetic information.

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

23 (b) Opportunity to Cure in Actions for Injunctive Relief.—

24 (1) NOTICE.—Subject to paragraph (3), an action for injunctive relief may be brought by  
25 an individual under this section only if, prior to initiating such action against an entity, the  
26 individual provides to the entity 30 days’ written notice identifying the specific provisions  
27 of this Act the individual alleges have been or are being violated.

28 (2) EFFECT OF CURE.—In the event a cure is possible, if, within the 30-day period, the  
29 entity cures the noticed violation and provides the individual with an express written  
30 statement that the violation has been cured and that no such further violation shall occur, an  
31 action for injunctive relief shall not be permitted.

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

35 (c) Notice of Actions Seeking Actual Damages.—

36 (1) NOTICE.—Subject to paragraph (2), an action for actual damages may be brought by  
37 an individual under this section only if, prior to initiating such action against an entity, the  
38 individuals provides to the entity 30 days’ written notice identifying the specific provisions  
39 of this Act the individual alleges have been or are being violated.

40 (2) SUBSTANTIAL PRIVACY HARM.—Notice shall not be required under paragraph (1) prior



1 to filing an action for actual damages for a violation of this Act that resulted in a substantial  
2 privacy harm if such action includes a claim for a preliminary injunction or temporary  
3 restraining order.

4 (d) Predispute Arbitration Agreements.—

5 (1) IN GENERAL.—Notwithstanding any other provision of law, at the election of the  
6 individual alleging a violation of this Act, no pre-dispute arbitration agreement shall be  
7 valid or enforceable with respect to—

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

9 (B) a claim alleging a violation that resulted in a substantial privacy harm.

10 (2) DETERMINATION OF APPLICABILITY.—Any issue as to whether this section applies to a  
11 dispute shall be determined under Federal law. The applicability of this section to an  
12 agreement to arbitrate and the validity and enforceability of an agreement to which this  
13 section applies shall be determined by a Federal court, rather than an arbitrator, irrespective  
14 of whether the party resisting arbitration challenges the arbitration agreement specifically or  
15 in conjunction with other terms of the contract containing such agreement, and irrespective  
16 of whether the agreement purports to delegate such determination to an arbitrator.

17 (3) DEFINITION OF PREDISPUTE ARBITRATION AGREEMENT.—For purposes of this  
18 subsection, the term “predispute arbitration agreement” means any agreement to arbitrate a  
19 dispute that has not arisen at the time of the making of the agreement.

20 (e) Clarification.—A person may combine the notices required by subsections (b)(1) and  
21 (c)(1) into a single notice if the single notice complies with the requirements of each subsection.

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

23 (a) Preemption of State Laws.—

24 (1) PURPOSES.—The purposes of this Act are to—

25 (A) establish a uniform national data privacy and data security standard in the  
26 United States to prevent administrative costs and burdens placed on interstate  
27 commerce; and

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

30 (2) IN GENERAL.—Except as provided in paragraph (3), no State or political subdivision  
31 thereof may adopt, maintain, enforce, or continue in effect any law, regulation, rule, or  
32 requirement covered by the provisions of this Act or a rule, regulation, or requirement  
33 promulgated under this Act.

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

36 (A) Consumer protection laws of general applicability, such as laws regulating  
37 deceptive, unfair, or unconscionable practices.

38 (B) Civil rights laws.

39 (C) Provisions of laws that address the privacy rights or other protections of

1 employees or employee information.

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

4 (E) Provision of laws that address notification requirements in the event of a data  
5 breach.

6 (F) Contract or tort law.

7 (G) Criminal laws unrelated to data privacy or data security.

8 (H) Criminal or civil laws regarding—

9 (i) blackmail;

10 (ii) stalking, including cyberstalking;

11 (iii) cyberbullying;

12 (iv) intimate images, including authentic or generated by a computer or by  
13 artificial intelligence, known to be nonconsensual;

14 (v) child abuse;

15 (vi) child sexual abuse material;

16 (vii) child abduction or attempted child abduction;

17 (viii) child trafficking; or

18 (ix) sexual harassment.

19 (I) Public safety or sector specific laws unrelated to data privacy or data security,  
20 provided that such laws do not directly conflict with the provisions of this Act.

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

23 (K) Provisions of laws that address banking records, financial records, tax records,  
24 social security numbers, credit cards, identity theft, credit reporting and investigations,  
25 credit repair, credit clinics, or check-cashing services.

26 (L) Provisions of laws that address electronic surveillance, wiretapping, telephone  
27 monitoring.

28 (M) Provisions of laws that address unsolicited email messages, telephone  
29 solicitation, or caller ID.

30 (N) Provisions of laws that protect the privacy of health information, healthcare  
31 information, medical information, medical records, HIV status, or HIV testing.

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

33 (P) Provisions of laws that address the use of encryption as a means of providing  
34 data security.

35 (b) Federal Law Preservation.—

36 (1) IN GENERAL.—Nothing in this Act or a regulation promulgated under this Act may be

1 construed to limit—

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

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

7 (C) any other provision of Federal law, except as otherwise provided in this Act.

8 (2) ANTITRUST SAVINGS CLAUSE.—

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

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

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

15 (B) RULE OF CONSTRUCTION.—Nothing in this Act, or the regulatory regime created  
16 under this Act, may be construed to modify, impair, supersede the operation of, or  
17 preclude the application of the antitrust laws.

18 (3) APPLICATION OF OTHER FEDERAL PRIVACY REQUIREMENTS.—

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

25 (B) LAWS AND REGULATIONS DESCRIBED.—For purposes of subparagraph (A), the  
26 laws and regulations described in this subparagraph are the following:

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

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

29 (iii) Subtitle D of the Health Information Technology for Economic and  
30 Clinical Health Act (42 U.S.C. 17931 et seq.).

31 (iv) The regulations promulgated pursuant to section 264(c) of the Health  
32 Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note).

33 (v) The requirements regarding the confidentiality of substance use disorder  
34 information under section 543 of the Public Health Service Act (42 U.S.C.  
35 290dd–2) or any regulation promulgated thereunder.

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

37 (vii) Section 444 of the General Education Provisions Act of 1974 (commonly  
38 known as the “Family Educational Rights and Privacy Act”) (20 U.S.C. 1232g)  
39 and part 99 of title 34, Code of Federal Regulations (or any successor regulation),

1 to the extent such covered entity or service provider is an educational agency or  
2 institution as defined in such section of such Act or section 99.3 of title 34, Code  
3 of Federal Regulations (or any successor regulation).

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

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

8 (A) IN GENERAL.—A covered entity or service provider that is required to comply  
9 with the laws and regulations described in subparagraph (B) and is in compliance with  
10 the information security requirements of such laws and regulations shall be deemed to  
11 be in compliance with section 9 of this Act, solely and exclusively with respect to any  
12 data subject to the requirements of such laws and regulations.

13 (B) LAWS AND REGULATIONS DESCRIBED.—For purposes of subparagraph (A), the  
14 laws and regulations described in this subparagraph are the following:

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

16 (ii) The Health Information Technology for Economic and Clinical Health Act  
17 (42 U.S.C. 17931 et seq.).

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

19 (iv) The regulations promulgated pursuant to section 264(c) of the Health  
20 Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note).

21 (C) IMPLEMENTATION GUIDANCE.—Not later than 1 year after the date of enactment  
22 of this Act, the Commission shall issue guidance regarding the implementation of this  
23 paragraph.

24 (c) Preservation of Common Law or Statutory Causes of Action for Civil Relief.—Nothing in  
25 this Act nor any amendment, standard, rule, requirement, assessment, law, or regulation  
26 promulgated under this Act shall be construed to preempt, displace, or supplant any Federal or  
27 State common law right or remedy, or any statute creating a remedy for civil relief, including any  
28 cause of action for personal injury, wrongful death, property damage, or other financial, physical,  
29 reputational, or psychological injury based in negligence, strict liability, products liability, failure  
30 to warn, or an objectively offensive intrusion into the private affairs or concerns of the  
31 individual, or any other legal theory of liability under any Federal or State common law, or any  
32 State statutory law, except that a violation of this Act or a regulation promulgated under this Act  
33 may not be pleaded as an element of any violation of such law.

34 (d) Non-application of Certain Provisions of the Communications Act of 1934.—

35 (1) IN GENERAL.—Notwithstanding any other provision of law, and except as provided in  
36 paragraph (2), the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts  
37 amendatory thereof or supplementary thereto and any regulation promulgated by the  
38 Federal Communications Commission under such an Act shall not apply to any covered  
39 entity or service provider with respect to the collection, processing, retention, transfer, or  
40 security of covered data to the extent that such collection, processing, retention, transfer, or  
41 security of covered data is governed by the requirements of this Act.

1 (2) EXCEPTIONS.—Paragraph (1) shall not preclude the application of any of the  
2 following to a covered entity or service provider with respect to the collection, processing,  
3 retention, transfer, or security of covered data:

4 (A) Subsections (b), (d), and (g) of section 222 of the Communications Act of 1934  
5 (47 U.S.C. 222).

6 (B) Section 64.2011 of title 47, Code of Federal Regulations (or any successor  
7 regulation).

8 (C) Mitigation measures and actions taken pursuant to Executive Order 13913 (85  
9 Fed. Reg. 19643; relating to the establishment of the Committee for the Assessment of  
10 Foreign Participation in the United States Telecommunications Services Sector).

11 (D) Any obligation under an international treaty related to the exchange of traffic  
12 implemented and enforced by the Federal Communications Commission.

## 13 SEC. 21. CHILDREN’S ONLINE PRIVACY PROTECTION 14 ACT OF 1998.

15 Nothing in this Act may be construed to relieve or change any obligation that a covered entity  
16 or other person may have under the Children’s Online Privacy Protection Act of 1998 (15 U.S.C.  
17 6501 et seq.).

## 18 SEC. 22. TERMINATION OF FTC RULEMAKING ON 19 COMMERCIAL SURVEILLANCE AND DATA SECURITY.

20 Beginning on the date of enactment of this Act, the Commission’s Trade Regulation Rule on  
21 Commercial Surveillance and Data Security proposed rulemaking, as published on August, 8,  
22 2022, shall be terminated.

## 23 SEC. 23. SEVERABILITY.

24 If any provision of this Act, or the application thereof to any person or circumstance, is held to  
25 be invalid, the remainder of this Act, and the application of such provision to other persons not  
26 similarly situated or to other circumstances, shall not be affected.

## 27 SEC. 24. EFFECTIVE DATE.

28 This Act shall take effect on the date that is 180 days after the date of enactment of the Act,  
29 unless otherwise specified in this Act.  
30