

116TH CONGRESS
1ST SESSION

S. _____

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

IN THE SENATE OF THE UNITED STATES

Ms. CANTWELL (for herself, Mr. SCHATZ, Ms. KLOBUCHAR, and Mr. MARKEY) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

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

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

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

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

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

Sec. 1. Short title; table of contents.

Sec. 2. Definitions.

Sec. 3. Effective date.

TITLE I—DATA PRIVACY RIGHTS

- Sec. 101. Duty of loyalty.
- Sec. 102. Right to access and transparency.
- Sec. 103. Right to delete.
- Sec. 104. Right to correct inaccuracies.
- Sec. 105. Right to controls.
- Sec. 106. Right to data minimization.
- Sec. 107. Right to data security.
- Sec. 108. Civil rights.
- Sec. 109. Prohibition on waiver of rights.
- Sec. 110. Limitations and applicability.

TITLE II—OVERSIGHT AND RESPONSIBILITY

- Sec. 201. Executive responsibility.
- Sec. 202. Privacy and data security officers; comprehensive privacy and data security programs; risk assessments and compliance.
- Sec. 203. Service providers and third parties.
- Sec. 204. Whistleblower protections.
- Sec. 205. Digital content forgeries.

TITLE III—MISCELLANEOUS

- Sec. 301. Enforcement, civil penalties, and applicability.
- Sec. 302. Relationship to Federal and State laws.
- Sec. 303. Severability.
- Sec. 304. Authorization of appropriations.

1 SEC. 2. DEFINITIONS.

2 In this Act:

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

4 (A) **IN GENERAL.**—The term “affirmative
 5 express consent” means an affirmative act by
 6 an individual that clearly communicates the in-
 7 dividual’s authorization for an act or practice,
 8 in response to a specific request that meets the
 9 requirements of subparagraph (B).

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

1 (i) The request is provided to the indi-
2 vidual in a standalone disclosure.

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

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

11 (II) is written in easy-to-under-
12 stand language and includes a promi-
13 nent heading that would enable a rea-
14 sonable individual to identify and un-
15 derstand the act or practice.

16 (iii) The request clearly explains the
17 individual's applicable rights related to
18 consent.

19 (C) EXPRESS CONSENT REQUIRED.—An
20 entity shall not infer that an individual has pro-
21 vided affirmative express consent to an act or
22 practice from the inaction of the individual or
23 the individual's continued use of a service or
24 product provided by the entity.

1 (2) ALGORITHMIC DECISION-MAKING.—The
2 term “algorithmic decision-making” means a com-
3 putational process, including one derived from ma-
4 chine learning, statistics, or other data processing or
5 artificial intelligence techniques that makes a deci-
6 sion or facilitates human decision making with re-
7 spect to covered data.

8 (3) BIOMETRIC INFORMATION.—

9 (A) IN GENERAL.—The term “biometric
10 information” means any covered data generated
11 from the measurement or specific technological
12 processing of an individual’s biological, physical,
13 or physiological characteristics, including—

- 14 (i) fingerprints;
15 (ii) voice prints;
16 (iii) iris or retina scans;
17 (iv) facial scans or templates;
18 (v) deoxyribonucleic acid (DNA) infor-
19 mation; and
20 (vi) gait.

21 (B) EXCLUSIONS.—Such term does not in-
22 clude writing samples, written signatures, pho-
23 tographs, voice recordings, demographic data,
24 or physical characteristics such as height,
25 weight, hair color, or eye color, provided that

1 such data is not used for the purpose of identi-
2 fying an individual’s unique biological, physical,
3 or physiological characteristics.

4 (4) COLLECT; COLLECTION.—The terms “col-
5 lect” and “collection” mean buying, renting, gath-
6 ering, obtaining, receiving, accessing, or otherwise
7 acquiring covered data by any means, including by
8 passively or actively observing the individual’s behav-
9 ior.

10 (5) COMMON BRANDING.—The term “common
11 branding” means a shared name, servicemark, or
12 trademark.

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

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

18 (B) control in any manner over the election
19 of a majority of the directors of the entity (or
20 of individuals exercising similar functions); or

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

23 (7) COMMISSION.—The term “Commission”
24 means the Federal Trade Commission.

25 (8) COVERED DATA.—

1 (A) IN GENERAL.—The term “covered
2 data” means information that identifies, or is
3 linked or reasonably linkable to an individual or
4 a consumer device, including derived data.

5 (B) EXCLUSIONS.—Such term does not in-
6 clude—

- 7 (i) de-identified data;
8 (ii) employee data; and
9 (iii) public records.

10 (9) COVERED ENTITY.—

11 (A) IN GENERAL.—The term “covered en-
12 tity” means any entity or person that—

- 13 (i) is subject to the Federal Trade
14 Commission Act (15 U.S.C. 41 et seq.);
15 and
16 (ii) processes or transfers covered
17 data.

18 (B) INCLUSION OF COMMONLY CON-
19 TROLLED AND COMMONLY BRANDED ENTI-
20 TIES.—Such term includes any entity or person
21 that controls, is controlled by, is under common
22 control with, or shares common branding with
23 a covered entity.

24 (C) EXCLUSION OF SMALL BUSINESS.—
25 Such term does not include a small business.

1 (10) DE-IDENTIFIED DATA.—Term “de-identi-
2 fied data” means information that cannot reasonably
3 be used to infer information about, or otherwise be
4 linked to, an individual, a household, or a device
5 used by an individual or household, provided that
6 the entity—

7 (A) takes reasonable measures to ensure
8 that the information cannot be reidentified, or
9 associated with, an individual, a household, or
10 a device used by an individual or household;

11 (B) publicly commits in a conspicuous
12 manner—

13 (i) to process and transfer the infor-
14 mation in a de-identified form; and

15 (ii) not to attempt to reidentify or as-
16 sociate the information with any individual,
17 household, or device used by an individual
18 or household; and

19 (C) contractually obligates any person or
20 entity that receives the information from the
21 covered entity to comply with all of the provi-
22 sions of this paragraph.

23 (11) DERIVED DATA.—The term “derived data”
24 means covered data that is created by the derivation
25 of information, data, assumptions, or conclusions

1 from facts, evidence, or another source of informa-
2 tion or data about an individual, household, or de-
3 vice used by an individual or household.

4 (12) EMPLOYEE DATA.—The term “employee
5 data” means—

6 (A) covered data that is collected by a cov-
7 ered entity or the covered entity’s service pro-
8 vider about an individual in the course of the
9 individual’s employment or application for em-
10 ployment (including on a contract or temporary
11 basis) provided that such data is retained or
12 processed by the covered entity or the covered
13 entity’s service provider solely for purposes nec-
14 essary for the individual’s employment or appli-
15 cation for employment;

16 (B) covered data that is collected by a cov-
17 ered entity or the covered entity’s service pro-
18 vider that is emergency contact information for
19 an individual who is an employee, contractor, or
20 job applicant of the covered entity provided that
21 such data is retained or processed by the cov-
22 ered entity or the covered entity’s service pro-
23 vider solely for the purpose of having an emer-
24 gency contact for such individual on file; and

1 (C) covered data that is collected by a cov-
2 ered entity or the covered entity's service pro-
3 vider about an individual (or a relative of an in-
4 dividual) who is an employee or former em-
5 ployee of the covered entity for the purpose of
6 administering benefits to which such individual
7 or relative is entitled on the basis of the individ-
8 ual's employment with the covered entity, pro-
9 vided that such data is retained or processed by
10 the covered entity or the covered entity's service
11 provider solely for the purpose of administering
12 such benefits.

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

16 (14) INDIVIDUAL.—The term “individual”
17 means a natural person residing in the United
18 States, however identified, including by any unique
19 identifier.

20 (15) LARGE DATA HOLDER.—The term “large
21 data holder” means a covered entity that, in the
22 most recent calendar year—

23 (A) processed or transferred the covered
24 data of more than 5,000,000 individuals, de-

1 vices used by individuals or households, or
2 households; or

3 (B) processed or transferred the sensitive
4 covered data of more than 100,000 individuals,
5 devices used by individuals or households, or
6 households.

7 (16) PROCESS.—The term “process” means
8 any operation or set of operations performed on cov-
9 ered data including collection, analysis, organization,
10 structuring, retaining, using, or otherwise handling
11 covered data.

12 (17) PROCESSING PURPOSE.—The term “proc-
13 essing purpose” means an adequately specific and
14 granular reason for which a covered entity processes
15 covered data that clearly describes the processing ac-
16 tivity.

17 (18) PUBLICLY AVAILABLE INFORMATION.—

18 (A) IN GENERAL.—The term “publicly
19 available information” means—

20 (i) information that a covered entity
21 has a reasonable basis to believe is lawfully
22 made available to the general public from
23 widely distributed media; and

24 (ii) information that is directly and
25 voluntarily disclosed to the general public

1 by the individual to whom the information
2 relates.

3 (B) LIMITATION.—Such term does not in-
4 clude—

5 (i) information derived from publicly
6 available information;

7 (ii) biometric information; or

8 (iii) nonpublicly available information
9 that has been combined with publicly avail-
10 able information.

11 (19) PUBLIC RECORDS.—The term “public
12 records” means information that is lawfully made
13 available from Federal, State, or local government
14 records provided that the covered entity processes
15 and transfers such information in accordance with
16 any restrictions or terms of use placed on the infor-
17 mation by the relevant government entity.

18 (20) SENSITIVE COVERED DATA.—The term
19 “sensitive covered data” means the following forms
20 of covered data:

21 (A) A government-issued identifier, such as
22 a Social Security number, passport number, or
23 driver’s license number.

24 (B) Any information that describes or re-
25 veals the past, present, or future physical

1 health, mental health, disability, or diagnosis of
2 an individual.

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

7 (D) Biometric information.

8 (E) Precise geolocation information that
9 reveals the past or present actual physical loca-
10 tion of an individual or device.

11 (F) The content or metadata of an individ-
12 ual's private communications or the identity of
13 the parties to such communications unless the
14 covered entity is an intended recipient of the
15 communication.

16 (G) An email address, telephone number,
17 or account log-in credentials.

18 (H) Information revealing an individual's
19 race, ethnicity, national origin, religion, or
20 union membership in a manner inconsistent
21 with the individual's reasonable expectation re-
22 garding disclosure of such information.

23 (I) Information revealing the sexual ori-
24 entation or sexual behavior of an individual in
25 a manner inconsistent with the individual's rea-

1 sonable expectation regarding disclosure of such
2 information.

3 (J) Information revealing online activities
4 over time and across third-party website or on-
5 line services.

6 (K) Calendar information, address book in-
7 formation, phone or text logs, photos, or videos
8 maintained on an individual's device.

9 (L) A photograph, film, video recording, or
10 other similar medium that shows the naked or
11 undergarment-clad private area of an indi-
12 vidual.

13 (M) Any other covered data processed or
14 transferred for the purpose of identifying the
15 above data types.

16 (N) Any other covered data that the Com-
17 mission determines to be sensitive covered data
18 through a rulemaking pursuant to section 553
19 of title 5, United States Code.

20 (21) SERVICE PROVIDER.—

21 (A) IN GENERAL.—The term “service pro-
22 vider” means a covered entity that processes or
23 transfers covered data in the course of per-
24 forming a service or function on behalf of, and
25 at the direction of, another covered entity, but

1 only to the extent that such processing or
2 transferral—

3 (i) relates to the performance of such
4 service or function; or

5 (ii) is necessary to comply with a legal
6 obligation or to establish, exercise, or de-
7 fend legal claims.

8 (B) EXCLUSION.—Such term does not in-
9 clude a covered entity that processes or trans-
10 fers the covered data outside of the direct rela-
11 tionship between the service provider and the
12 covered entity.

13 (22) SERVICE PROVIDER DATA.—The term
14 “service provider data” means covered data that is
15 collected by or has been transferred to a service pro-
16 vider by a covered entity for the purpose of allowing
17 the service provider to perform a service or function
18 on behalf of, and at the direction of, such covered
19 entity.

20 (23) SMALL BUSINESS.—

21 (A) IN GENERAL.—The term “small busi-
22 ness” means an entity that can establish that,
23 with respect to the 3 preceding calendar years
24 (or for the period during which the entity has

1 been in existence if, as of such date, such pe-
2 riod is less than 3 years) the entity does not—

3 (i) maintain annual average gross rev-
4 enue in excess of \$25,000,000;

5 (ii) annually process the covered data
6 of an average of 100,000 or more individ-
7 uals, households, or devices used by indi-
8 viduals or households; and

9 (iii) derive 50 percent or more of its
10 annual revenue from transferring individ-
11 uals' covered data.

12 (B) COMMON CONTROL; COMMON BRAND-
13 ING.—For purposes of subparagraph (A), the
14 annual average gross revenue, data processing
15 volume, and percentage of annual revenue of an
16 entity shall include the revenue and processing
17 activities of any person that controls, is con-
18 trolled by, is under common control with, or
19 shares common branding with such entity.

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

21 (A) means any person or entity that—

22 (i) processes or transfers third party
23 data; and

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

1 (B) does not include a person or entity
2 that collects covered data from another entity if
3 the two entities are related by common owner-
4 ship or corporate control and share common
5 branding.

6 (25) THIRD PARTY DATA.—The term “third
7 party data” means covered data that is transferred
8 to a third party by a covered entity.

9 (26) TRANSFER.—The term “transfer” means
10 to disclose, release, share, disseminate, make avail-
11 able, sell, license, or otherwise communicate covered
12 data by any means to a service provider or third
13 party—

14 (A) in exchange for consideration; or

15 (B) for a commercial purpose.

16 (27) UNIQUE IDENTIFIER.—The term “unique
17 identifier” means an identifier that is reasonably
18 linkable to an individual, household, or device used
19 by an individual or household, including a device
20 identifier, an Internet Protocol address, cookies, bea-
21 cons, pixel tags, mobile ad identifiers, or similar
22 technology, customer number, unique pseudonym, or
23 user alias, telephone numbers, or other forms of per-
24 sistent or probabilistic identifiers that can be used to

1 identify a particular individual, a household, or a de-
2 vice.

3 (28) WIDELY DISTRIBUTED MEDIA.—The term
4 “widely distributed media” means information that
5 is available to the general public, including informa-
6 tion from a telephone book or online directory, a tel-
7 evision, internet, or radio program, the news media,
8 or an internet site that is available to the general
9 public on an unrestricted basis, but does not include
10 an obscene visual depiction as defined in section
11 1460 of title 18, United States Code.

12 **SEC. 3. EFFECTIVE DATE.**

13 This Act shall take effect on the date that is 180 days
14 after the date of enactment of this Act.

15 **TITLE I—DATA PRIVACY RIGHTS**

16 **SEC. 101. DUTY OF LOYALTY.**

17 (a) IN GENERAL.—A covered entity shall not—

18 (1) engage in a deceptive data practice or a
19 harmful data practice; or

20 (2) process or transfer covered data in a man-
21 ner that violates any provision of this Act.

22 (b) DEFINITIONS.—

23 (1) DECEPTIVE DATA PRACTICE.—The term
24 “deceptive data practice” means an act or practice
25 involving the processing or transfer of covered data

1 in a manner that constitutes a deceptive act or prac-
2 tice in violation of section 5(a)(1) of the Federal
3 Trade Commission Act (15 U.S.C. 45(a)(1)).

4 (2) HARMFUL DATA PRACTICE.—The term
5 “harmful data practice” means the processing or
6 transfer of covered data in a manner that causes or
7 is likely to cause any of the following:

8 (A) Financial, physical, or reputational in-
9 jury to an individual.

10 (B) Physical or other offensive intrusion
11 upon the solitude or seclusion of an individual
12 or the individual’s private affairs or concerns,
13 where such intrusion would be offensive to a
14 reasonable person.

15 (C) Other substantial injury to an indi-
16 vidual.

17 **SEC. 102. RIGHT TO ACCESS AND TRANSPARENCY.**

18 (a) RIGHT TO ACCESS.—A covered entity, upon the
19 verified request of an individual, shall provide the indi-
20 vidual, in a human-readable format that a reasonable indi-
21 vidual can understand, with—

22 (1) a copy or accurate representation of the
23 covered data of the individual processed or trans-
24 ferred by the covered entity; and

1 (2) the name of any third party to whom cov-
2 ered data of the individual has been transferred by
3 the covered entity and a description of the purpose
4 for which the entity transferred such data to such
5 third party.

6 (b) RIGHT TO TRANSPARENCY.—A covered entity
7 shall make publicly and persistently available, in a con-
8 spicuous and readily accessible manner, a privacy policy
9 that provides a detailed and accurate representation of the
10 entity’s data processing and data transfer activities. Such
11 privacy policy shall include, at a minimum—

12 (1) the identity and the contact information of
13 the covered entity, including the contact information
14 for the covered entity’s representative for privacy
15 and data security inquiries;

16 (2) each category of data the covered entity col-
17 lects and the processing purposes for which such
18 data is collected;

19 (3) whether the covered entity transfers covered
20 data and, if so—

21 (A) each category of service provider and
22 third party to which the covered entity transfers
23 covered data and the purposes for which such
24 data is transferred to such categories; and

1 (B) the identity of each third party to
2 which the covered entity transfers covered data
3 and the purposes for which such data is trans-
4 ferred to such third party, except for transfers
5 to governmental entities pursuant to a court
6 order or law that prohibits the covered entity
7 from disclosing such transfer;

8 (4) how long covered data processed by the cov-
9 ered entity will be retained by the covered entity and
10 a description of the covered entity's data minimiza-
11 tion policies;

12 (5) how individuals can exercise the individual
13 rights described in this title;

14 (6) a description of the covered entity's data se-
15 curity policies; and

16 (7) the effective date of the privacy policy.

17 (c) LANGUAGES.—A covered entity shall make the
18 privacy policy required under this section available to the
19 public in all of the languages in which the covered entity
20 provides a product or service or carries out any other ac-
21 tivities to which the privacy policy relates.

22 (d) RIGHT TO CONSENT TO MATERIAL CHANGES.—
23 A covered entity shall not make a material change to its
24 privacy policy or practices with respect to previously col-
25 lected covered data that would weaken the privacy protec-

1 tions applicable to such data without first obtaining prior
2 affirmative express consent from the individuals affected.
3 The covered entity shall provide direct notification, where
4 possible, regarding material changes to affected individ-
5 uals, taking into account available technology and the na-
6 ture of the relationship.

7 **SEC. 103. RIGHT TO DELETE.**

8 A covered entity, upon the verified request of an indi-
9 vidual, shall—

10 (1) delete, or allow the individual to delete, any
11 information in the covered data of the individual
12 that is processed by the covered entity; and

13 (2) inform any service provider or third party
14 to which the covered entity transferred such data of
15 the individual's deletion request.

16 **SEC. 104. RIGHT TO CORRECT INACCURACIES.**

17 A covered entity, upon the verified request of an indi-
18 vidual, shall—

19 (1) correct, or allow the individual to correct,
20 inaccurate or incomplete information in the covered
21 data of the individual that is processed by the cov-
22 ered entity; and

23 (2) inform any service provider or third party
24 to which the covered entity transferred such data of
25 the corrected information.

1 **SEC. 105. RIGHT TO CONTROLS.**

2 (a) **RIGHT TO DATA PORTABILITY.**—A covered enti-
3 ty, upon the verified request of an individual, shall export
4 the individual’s covered data, except for derived data,
5 without licensing restrictions—

6 (1) in a human-readable format that allows the
7 individual to understand such covered data of the in-
8 dividual; and

9 (2) in a structured, interoperable, and machine-
10 readable format that includes all covered data or
11 other information that the covered entity collected to
12 the extent feasible.

13 (b) **RIGHT TO OPT OUT OF TRANSFERS.**—

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

15 (A) shall not transfer an individual’s cov-
16 ered data to a third party if the individual ob-
17 jects to the transfer; and

18 (B) shall allow an individual to object to
19 the covered entity transferring covered data of
20 the individual to a third party through a proc-
21 ess established under the rule issued by the
22 Commission pursuant to paragraph (2).

23 (2) **RULEMAKING.**—

24 (A) **IN GENERAL.**—Not later than 18
25 months after the date of enactment of this Act,
26 the Commission shall issue a rule under section

1 553 of title 5, United States Code, establishing
2 one or more acceptable processes for covered
3 entities to follow in allowing individuals to opt
4 out of transfers of covered data.

5 (B) REQUIREMENTS.—The processes es-
6 tablished by the Commission pursuant to this
7 subparagraph shall—

8 (i) be centralized, to the extent fea-
9 sible, to minimize the number of opt-out
10 designations of a similar type that a con-
11 sumer must make;

12 (ii) include clear and conspicuous opt-
13 out notices and consumer friendly mecha-
14 nisms to allow an individual to opt out of
15 transfers of covered data;

16 (iii) allow an individual that objects to
17 a transfer of covered data to view the sta-
18 tus of such objection;

19 (iv) allow an individual that objects to
20 a transfer of covered data to change the
21 status of such objection;

22 (v) be privacy protective; and

23 (vi) be informed by the Commission's
24 experience developing and implementing
25 the National Do Not Call Registry.

1 (c) SENSITIVE DATA.—A covered entity—

2 (1) shall not process the sensitive covered data
3 of an individual without the individual’s prior, af-
4 firmative express consent;

5 (2) shall not transfer the sensitive covered data
6 of an individual without the individual’s prior, af-
7 firmative express consent;

8 (3) shall provide an individual with a consumer-
9 friendly means to withdraw affirmative express con-
10 sent to process the sensitive covered data of the indi-
11 vidual; and

12 (4) is not required to obtain prior, affirmative
13 express consent to process or transfer publicly avail-
14 able information.

15 **SEC. 106. RIGHT TO DATA MINIMIZATION.**

16 A covered entity shall not process or transfer covered
17 data beyond what is reasonably necessary, proportionate,
18 and limited—

19 (1) to carry out the specific processing purposes
20 and transfers described in the privacy policy made
21 available by the covered entity as required under sec-
22 tion 102;

23 (2) to carry out a specific processing purpose or
24 transfer for which the covered entity has obtained
25 affirmative express consent; or

1 (3) for a purpose specifically permitted under
2 subsection (d) of section 110.

3 Covered data processing and transfers consistent with this
4 section shall not supersede any other provision of this Act.

5 **SEC. 107. RIGHT TO DATA SECURITY.**

6 (a) IN GENERAL.—A covered entity shall establish,
7 implement, and maintain reasonable data security prac-
8 tices to protect the confidentiality, integrity, and accessi-
9 bility of covered data. Such data security practices shall
10 be appropriate to the volume and nature of the covered
11 data at issue.

12 (b) SPECIFIC REQUIREMENTS.—Data security prac-
13 tices required under subsection (a) shall include, at a min-
14 imum, the following:

15 (1) ASSESS VULNERABILITIES.—Identifying
16 and assessing any reasonably foreseeable risks to,
17 and vulnerabilities in, each system maintained by
18 the covered entity that processes or transfers cov-
19 ered data, including unauthorized access to or risks
20 to covered data, human vulnerabilities, access rights,
21 and use of service providers. Such activities shall in-
22 clude a plan to receive and respond to unsolicited re-
23 ports of vulnerabilities by entities and individuals.

24 (2) PREVENTIVE AND CORRECTION ACTION.—
25 Taking preventive and corrective action to mitigate

1 any risks or vulnerabilities to covered data identified
2 by the covered entity, which may include imple-
3 menting administrative, technical, or physical safe-
4 guards or changes to data security practices or the
5 architecture, installation, or implementation of net-
6 work or operating software.

7 (3) INFORMATION RETENTION AND DIS-
8 POSAL.—Disposing covered data that is required to
9 be deleted or is no longer necessary for the purpose
10 for which the data was collected unless an individual
11 has provided affirmative express consent to such re-
12 tention. Such process shall include destroying, per-
13 manently erasing, or otherwise modifying the cov-
14 ered data to make such data permanently
15 unreadable or indecipherable and unrecoverable and
16 data hygiene practices to ensure ongoing compliance
17 with this subsection.

18 (4) TRAINING.—Training all employees with ac-
19 cess to covered data on how to safeguard covered
20 data and protect individual privacy and updating
21 that training as necessary.

22 (c) TRAINING GUIDELINES.—Not later than 1 year
23 after the date of enactment of this Act, the Commission,
24 in conjunction with the National Institute of Standards
25 and Technology, shall publish guidance for covered entities

1 on how to provide effective data security and privacy train-
2 ing as described in subsection (b)(4).

3 **SEC. 108. CIVIL RIGHTS.**

4 (a) PROTECTIONS.—

5 (1) IN GENERAL.—A covered entity shall not
6 process or transfer covered data on the basis of an
7 individual's or class of individuals' actual or per-
8 ceived race, color, ethnicity, religion, national origin,
9 sex, gender, gender identity, sexual orientation, fa-
10 miliary status, biometric information, lawful source of
11 income, or disability—

12 (A) for the purpose of advertising, mar-
13 keting, soliciting, offering, selling, leasing, li-
14 censing, renting, or otherwise commercially con-
15 tracting for a housing, employment, credit, or
16 education opportunity, in a manner that unlaw-
17 fully discriminates against or otherwise makes
18 the opportunity unavailable to the individual or
19 class of individuals; or

20 (B) in a manner that unlawfully seg-
21 regates, discriminates against, or otherwise
22 makes unavailable to the individual or class of
23 individuals the goods, services, facilities, privi-
24 leges, advantages, or accommodations of any
25 place of public accommodation.

1 (2) EXCEPTION.—Nothing in this section shall
2 limit a covered entity from processing covered data
3 for legitimate internal testing for the purpose of pre-
4 venting unlawful discrimination or otherwise deter-
5 mining the extent or effectiveness of the covered en-
6 tity’s compliance with this Act.

7 (3) FTC ADVISORY OPINIONS.—A covered enti-
8 ty may request advice from the Commission con-
9 cerning the covered entity’s potential compliance
10 with this subsection, in accordance with the Com-
11 mission’s rules of practice on advisory opinions.

12 (b) ALGORITHMIC DECISION-MAKING IMPACT AS-
13 SESSMENT.—

14 (1) IMPACT ASSESSMENT.—Notwithstanding
15 any other provision of law, a covered entity engaged
16 in algorithmic decision-making, or in assisting others
17 in algorithmic decision-making for the purpose of
18 processing or transferring covered data, solely or in
19 part to make or facilitate advertising for housing,
20 education, employment or credit opportunities, or an
21 eligibility determination for housing, education, em-
22 ployment or credit opportunities or determining ac-
23 cess to, or restrictions on the use of, any place of
24 public accommodation, must annually conduct an

1 impact assessment of such algorithmic decision-mak-
2 ing that—

3 (A) describes and evaluates the develop-
4 ment of the covered entity’s algorithmic deci-
5 sion-making processes including the design and
6 training data used to develop the algorithmic
7 decision-making process, how the algorithmic
8 decision-making process was tested for accu-
9 racy, fairness, bias and discrimination; and

10 (B) assesses whether the algorithmic deci-
11 sion-making system produces discriminatory re-
12 sults on the basis of an individual’s or class of
13 individuals’ actual or perceived race, color, eth-
14 nicity, religion, national origin, sex, gender,
15 gender identity, sexual orientation, familial sta-
16 tus, biometric information, lawful source of in-
17 come, or disability.

18 (2) **EXTERNAL, INDEPENDENT AUDITOR OR RE-**
19 **SEARCHER.**—A covered entity may utilize an exter-
20 nal, independent auditor or researcher to conduct
21 such assessments.

22 (3) **AVAILABILITY.**—The covered entity—

23 (A) shall make the impact assessment
24 available to the Commission upon request; and

1 (B) may make the impact assessment pub-
2 lic.

3 A covered entity may redact and segregate trade se-
4 crets as defined by section 1839 of title 18, United
5 States Code, from public disclosure under this sub-
6 section.

7 (4) STUDY.—Not later than 3 years after the
8 date of enactment of this Act, the Commission shall
9 publish a report containing the results of a study,
10 using the Commission’s authority under section 6(b)
11 of the Federal Trade Commission Act (15 U.S.C.
12 46(b)), examining the use of algorithms for the pur-
13 poses described in this subsection. Not later than 3
14 years after the publication of the initial report, and
15 as necessary thereafter, the Commission shall pub-
16 lish a new and updated version of such report.

17 **SEC. 109. PROHIBITION ON WAIVER OF RIGHTS.**

18 A covered entity shall not condition the provision of
19 a service or product to an individual on the individual’s
20 agreement to waive privacy rights guaranteed by—

21 (1) sections 101, 105(a), and 106 through 109
22 of this Act; and

23 (2) sections 102 through 104, and 105(b) and
24 (c) of this Act, except in the case where—

1 (A) there exists a direct relationship be-
2 tween the individual and the covered entity ini-
3 tiated by the individual;

4 (B) the provision of the service or product
5 requested by the individual requires the proc-
6 essing or transferring of the specific covered
7 data of the individual and the covered data is
8 strictly necessary to provide the service or prod-
9 uct; and

10 (C) an individual provides affirmative ex-
11 press consent to such specific limitations.

12 **SEC. 110. LIMITATIONS AND APPLICABILITY.**

13 (a) VERIFICATION OF REQUESTS.—

14 (1) IN GENERAL.—A covered entity shall not
15 permit an individual to exercise a right described in
16 sections 102 through 105(a) if—

17 (A) the covered entity cannot reasonably
18 verify that the individual making the request to
19 exercise the right is the individual whose cov-
20 ered data is the subject of the request or an in-
21 dividual authorized to make such a request on
22 the individual's behalf; or

23 (B) the covered entity reasonably believes
24 that the request is made to interfere with a

1 contract between the covered entity and another
2 individual.

3 (2) ADDITIONAL INFORMATION.—If a covered
4 entity cannot reasonably verify that a request to ex-
5 ercise a right described in sections 102 through
6 105(a) is made by the individual whose covered data
7 is the subject of the request (or an individual au-
8 thorized to make such a request on the individual’s
9 behalf), the covered entity shall request the provision
10 of additional information necessary for the sole pur-
11 pose of verifying the identity of the individual and
12 shall not process or transfer such additional infor-
13 mation for any other purpose.

14 (3) BURDEN MINIMIZATION.—A covered entity
15 shall minimize the inconvenience to consumers relat-
16 ing to the verification or authentication of requests.

17 (b) COST OF ACCESS.—A covered entity shall carry
18 out the rights described in sections 102 through 105(a)
19 free of charge.

20 (c) EXCEPTIONS TO SECTIONS 102 THROUGH
21 105(b).—A covered entity may decline to comply with an
22 individual’s request to exercise a right described in sec-
23 tions 102 through 105(b) if—

24 (1) complying with the request would be demon-
25 strably impossible (for purposes of this paragraph,

1 the receipt of a large number of verified requests, on
2 its own, shall not be considered to render compliance
3 with a request demonstrably impossible);

4 (2) complying with the request would prevent
5 the covered entity from carrying out internal audits,
6 performing accounting functions, processing refunds,
7 or fulfilling warranty claims, provided that the cov-
8 ered data that is the subject of the request is not
9 processed or transferred for any purpose other than
10 such specific activities;

11 (3) the request is made to correct or delete pub-
12 licly available information, and then only to the ex-
13 tent the data is publicly available information;

14 (4) complying with the request would impair
15 the publication of newsworthy information of legiti-
16 mate public concern to the public by a covered enti-
17 ty, or the processing or transfer of information by
18 a covered entity for such purpose;

19 (5) complying with the request would impair
20 the privacy of another individual or the rights of an-
21 other to exercise free speech; or

22 (6) the covered entity processes or will process
23 the data subject to the request for a specific purpose
24 described in subsection (d) of this section, and com-
25 plying with the request would prevent the covered

1 entity from using such data for such specific pur-
2 pose.

3 (d) EXCEPTIONS TO AFFIRMATIVE EXPRESS CON-
4 SENT.—

5 (1) IN GENERAL.—A covered entity may proc-
6 ess or transfer covered data without the individual’s
7 affirmative express consent for any of the following
8 purposes, provided that the processing or transfer is
9 reasonably necessary, proportionate, and limited to
10 such purpose:

11 (A) To complete a transaction or fulfill an
12 order or service specifically requested by an in-
13 dividual, such as billing, shipping, or account-
14 ing.

15 (B) To perform system maintenance,
16 debug systems, or repair errors to ensure the
17 functionality of a product or service provided by
18 the covered entity.

19 (C) To detect or respond to a security inci-
20 dent, provide a secure environment, or maintain
21 the safety of a product or service.

22 (D) To protect against malicious, decep-
23 tive, fraudulent or illegal activity.

1 (E) To comply with a legal obligation or
2 the establishment, exercise, or defense of legal
3 claims.

4 (F) To prevent an individual from suf-
5 fering harm where the covered entity believes in
6 good faith that the individual is in danger of
7 suffering death or serious physical injury.

8 (G) To effectuate a product recall pursu-
9 ant to Federal or State law.

10 (H) To conduct scientific, historical, or
11 statistical research in the public interest that
12 adheres to all other applicable ethics and pri-
13 vacy laws and is approved, monitored, and gov-
14 erned by an institutional review board or a
15 similar oversight entity that meets standards
16 promulgated by the Commission pursuant to
17 section 553 of title 5, United States Code.

18 (2) BIOMETRIC INFORMATION.—Not later than
19 1 year after the date of enactment of this Act, the
20 Commission shall promulgate regulations pursuant
21 to section 553 of title 5, United States Code, identi-
22 fying privacy protective requirements for the proc-
23 essing of biometric information for a purpose de-
24 scribed in subparagraph (C) or (D) of paragraph
25 (1). Such regulations shall include—

1 (A) strict data processing limitations, in-
2 cluding a prohibition on the processing of bio-
3 metric information unless the covered entity has
4 a reasonable suspicion, after a specific criminal
5 incident involving the covered entity, that the
6 individual may engage in criminal activity;

7 (B) strict data transfer limitations, includ-
8 ing a prohibition on the transfer of biometric
9 information to a third party other than to com-
10 ply with a legal obligation or to establish, exer-
11 cise, or defend a legal claim; and

12 (C) strict transparency obligations, includ-
13 ing requiring disclosures in a conspicuous and
14 readily accessible manner regarding specific
15 data processing and transfer activities.

16 (e) JOURNALISM EXCEPTION.—Nothing in this title
17 shall apply to the publication of newsworthy information
18 of legitimate public concern to the public by a covered en-
19 tity, or to the processing or transfer of information by a
20 covered entity for that purpose.

21 (f) APPLICABILITY OF OTHER DATA PRIVACY RE-
22 QUIREMENTS.—A covered entity that is required to com-
23 ply with title V of the Gramm-Leach-Bliley Act (15 U.S.C.
24 6801 et seq.), the Health Information Technology for Eco-
25 nomic and Clinical Health Act (42 U.S.C. 17931 et seq.),

1 part C of title XI of the Social Security Act (42 U.S.C.
2 1320d et seq.), the Fair Credit Reporting Act (15 U.S.C.
3 1681 et seq.), the Family Educational Rights and Privacy
4 Act (20 U.S.C. 1232g; part 99 of title 34, Code of Federal
5 Regulations), or the regulations promulgated pursuant to
6 section 264(c) of the Health Insurance Portability and Ac-
7 countability Act of 1996 (42 U.S.C. 1320d–2 note), and
8 is in compliance with the data privacy requirements of
9 such regulations, part, title, or Act (as applicable), shall
10 be deemed to be in compliance with the related require-
11 ments of this title, except for section 107, with respect
12 to data subject to the requirements of such regulations,
13 part, title, or Act. Not later than 1 year after the date
14 of enactment of this Act, the Commission shall issue guid-
15 ance describing the implementation of this subsection.

16 (g) **APPLICABILITY OF OTHER DATA SECURITY RE-**
17 **QUIREMENTS.**—A covered entity that is required to com-
18 ply with title V of the Gramm-Leach-Bliley Act (15 U.S.C.
19 6801 et seq.), the Health Information Technology for Eco-
20 nomic and Clinical Health Act (42 U.S.C. 17931 et seq.),
21 part C of title XI of the Social Security Act (42 U.S.C.
22 1320d et seq.), or the regulations promulgated pursuant
23 to section 264(c) of the Health Insurance Portability and
24 Accountability Act of 1996 (42 U.S.C. 1320d–2 note), and
25 is in compliance with the information security require-

1 ments of such regulations, part, title, or Act (as applica-
2 ble), shall be deemed to be in compliance with the require-
3 ments of section 107 with respect to data subject to the
4 requirements of such regulations, part, title, or Act. Not
5 later than 1 year after the date of enactment of this Act,
6 the Commission shall issue guidance describing the imple-
7 mentation of this subsection.

8 (h) IN GENERAL.—The Commission shall have au-
9 thority under section 553 of title 5, United States Code,
10 to promulgate regulations necessary to carry out the provi-
11 sions of this title.

12 **TITLE II—OVERSIGHT AND** 13 **RESPONSIBILITY**

14 **SEC. 201. EXECUTIVE RESPONSIBILITY.**

15 (a) IN GENERAL.—Beginning 1 year after the date
16 of enactment of this Act, the chief executive officer of a
17 covered entity that is a large data holder (or, if the entity
18 does not have a chief executive officer, the highest ranking
19 officer of the entity) and each privacy officer and data se-
20 curity officer of such entity shall annually certify to the
21 Commission, in a manner specified by the Commission,
22 that the entity maintains—

23 (1) adequate internal controls to comply with
24 this Act; and

1 (2) reporting structures to ensure that such
2 certifying officers are involved in, and are respon-
3 sible for, decisions that impact the entity's compli-
4 ance with this Act.

5 (b) REQUIREMENTS.—A certification submitted
6 under subsection (a) shall be based on a review of the ef-
7 fectiveness of a covered entity's internal controls and re-
8 porting structures that is conducted by the certifying offi-
9 cers no more than 90 days before the submission of the
10 certification.

11 **SEC. 202. PRIVACY AND DATA SECURITY OFFICERS; COM-**
12 **PREHENSIVE PRIVACY AND DATA SECURITY**
13 **PROGRAMS; RISK ASSESSMENTS AND COM-**
14 **PLIANCE.**

15 (a) PRIVACY AND DATA SECURITY OFFICER.—A cov-
16 ered entity shall designate—

17 (1) 1 or more qualified employees as privacy of-
18 ficers; and

19 (2) 1 or more qualified employees (in addition
20 to any employee designated under paragraph (1)) as
21 data security officers.

22 (b) COMPREHENSIVE PRIVACY AND DATA SECURITY
23 PROGRAMS, RISK ASSESSMENTS, AND COMPLIANCE.—An
24 employee who is designated by a covered entity as a pri-

1 vacy officer or a data security officer shall be responsible
2 for, at a minimum—

3 (1) implementing a comprehensive written data
4 privacy program and data security program to safe-
5 guard the privacy and security of covered data
6 throughout the life cycle of development and oper-
7 ational practices of the covered entity's products or
8 services;

9 (2) annually conducting privacy and data secu-
10 rity risk assessments, data hygiene, and other qual-
11 ity control practices; and

12 (3) facilitating the covered entity's ongoing
13 compliance with this Act.

14 **SEC. 203. SERVICE PROVIDERS AND THIRD PARTIES.**

15 (a) SERVICE PROVIDERS.—A service provider—

16 (1) shall not process service provider data for
17 any processing purpose other than one performed on
18 behalf of, and at the direction of, the covered entity
19 that transferred such data to the service provider,
20 except that a service provider may process data to
21 comply with a legal obligation or the establishment,
22 exercise, or defense of legal claims;

23 (2) shall not transfer service provider data to a
24 third party without the affirmative express consent,
25 obtained by, or on behalf of, the covered entity, of

1 the individual to whom the service provider data is
2 linked or reasonably linkable;

3 (3) shall delete or de-identify service provider
4 data after the agreed upon end of the provision of
5 services;

6 (4) is exempt from the requirements of sections
7 102(a), 103, 104, and 105(a) with respect to service
8 provider data, but shall, to the extent practicable—

9 (A) assist the covered entity from which it
10 received the service provider data in fulfilling
11 requests made by individuals under such sec-
12 tions; and

13 (B) shall delete, de-identify, or correct (as
14 applicable), any service provider data that is
15 subject to a verified request from an individual
16 described in section 103 or 104; and

17 (5) is exempt from the requirements of section
18 106 with respect to service provider data, but shall
19 have the same responsibilities and obligations as a
20 covered entity with respect to such data under all
21 other provisions of this Act.

22 (b) THIRD PARTIES.—A third party—

23 (1) shall not process third party data for a pur-
24 pose that is inconsistent with the expectations of a
25 reasonable individual;

1 (2) may reasonably rely on representations
2 made by the covered entity that transferred third
3 party data regarding the expectation of a reasonable
4 individual, provided the third party conducts reason-
5 able due diligence on the representations of the cov-
6 ered entity and finds those representations to be
7 credible; and

8 (3) upon receipt of any third party data, is ex-
9 empt from the requirements of section 105(c) with
10 respect to such data, but shall have the same re-
11 sponsibilities and obligations as a covered entity with
12 respect to such data under all other provisions of
13 this Act.

14 (c) ADDITIONAL OBLIGATIONS ON COVERED ENTI-
15 TIES.—

16 (1) IN GENERAL.—A covered entity shall—

17 (A) exercise reasonable due diligence in se-
18 lecting a service provider and conduct reason-
19 able oversight of its service providers to ensure
20 compliance with the applicable requirements of
21 this section; and

22 (B) exercise reasonable due diligence in de-
23 ciding to transfer covered data to a third party,
24 and conduct oversight of third parties to which

1 it transfers data to ensure compliance with the
2 applicable requirements of this subsection.

3 (2) GUIDANCE.—Not later than 1 year after
4 the date of enactment of this Act, the Commission
5 shall issue guidance for covered entities regarding
6 compliance with this subsection.

7 (d) IN GENERAL.—The Commission shall have au-
8 thority under section 553 of title 5, United States Code,
9 to promulgate regulations necessary to carry out the provi-
10 sions of this section.

11 **SEC. 204. WHISTLEBLOWER PROTECTIONS.**

12 (a) IN GENERAL.—A covered entity shall not, directly
13 or indirectly, discharge, demote, suspend, threaten, har-
14 ass, or in any other manner discriminate against a covered
15 individual of the covered entity because—

16 (1) the covered individual, or anyone perceived
17 as assisting the covered individual, takes (or the cov-
18 ered entity suspects that the covered individual has
19 taken or will take) a lawful action in providing to
20 the Federal Government or the attorney general of
21 a State information relating to any act or omission
22 that the covered individual reasonably believes to be
23 a violation of this Act or any regulation promulgated
24 under this Act;

1 (2) the covered individual provides information
2 that the covered individual reasonably believes evi-
3 dences such a violation to—

4 (A) a person with supervisory authority
5 over the covered individual at the covered enti-
6 ty; or

7 (B) another individual working for the cov-
8 ered entity who the covered individual reason-
9 ably believes has the authority to investigate,
10 discover, or terminate the violation or to take
11 any other action to address the violation;

12 (3) the covered individual testifies (or the cov-
13 ered entity expects that the covered individual will
14 testify) in an investigation or judicial or administra-
15 tive proceeding concerning such a violation; or

16 (4) the covered individual assists or participates
17 (or the covered entity expects that the covered indi-
18 vidual will assist or participate) in such an investiga-
19 tion or judicial or administrative proceeding, or the
20 covered individual takes any other action to assist in
21 carrying out the purposes of this Act.

22 (b) ENFORCEMENT.—An individual who alleges dis-
23 charge or other discrimination in violation of subsection
24 (a) may bring an action governed by the rules, procedures,
25 statute of limitations, and legal burdens of proof in section

1 42121(b) of title 49, United States Code. If the individual
2 has not received a decision within 180 days and there is
3 no showing that such delay is due to the bad faith of the
4 claimant, the individual may bring an action for a jury
5 trial, governed by the burden of proof in section 42121(b)
6 of title 49, United States Code, in the appropriate district
7 court of the United States for the following relief:

8 (1) Temporary relief while the case is pending.

9 (2) Reinstatement with the same seniority sta-
10 tus that the individual would have had, but for the
11 discharge or discrimination.

12 (3) Three times the amount of back pay other-
13 wise owed to the individual, with interest.

14 (4) Consequential and compensatory damages,
15 and compensation for litigation costs, expert witness
16 fees, and reasonable attorneys' fees.

17 (c) WAIVER OF RIGHTS AND REMEDIES.—The rights
18 and remedies provided for in this section shall not be
19 waived by any policy form or condition of employment, in-
20 cluding by a predispute arbitration agreement.

21 (d) PREDISPUTE ARBITRATION AGREEMENTS.—No
22 predispute arbitration agreement shall be valid or enforce-
23 able if the agreement requires arbitration of a dispute
24 arising under this section.

1 (e) COVERED INDIVIDUAL DEFINED.—In this sec-
2 tion, the term “covered individual” means an applicant,
3 current or former employee, contractor, subcontractor,
4 grantee, or agent of an employer.

5 **SEC. 205. DIGITAL CONTENT FORGERIES.**

6 (a) REPORTS.—Not later than 1 year after the date
7 of enactment of this Act, and annually thereafter, the Di-
8 rector of the National Institute of Standards and Tech-
9 nology shall publish a report regarding digital content for-
10 geries.

11 (b) REQUIREMENTS.—Each report under subsection
12 (a) shall include the following:

13 (1) A definition of digital content forgeries
14 along with accompanying explanatory materials. The
15 definition developed pursuant to this section shall
16 not supersede any other provision of law or be con-
17 strued to limit the authority of any executive agency
18 related to digital content forgeries.

19 (2) A description of the common sources in the
20 United States of digital content forgeries and com-
21 mercial sources of digital content forgery tech-
22 nologies.

23 (3) An assessment of the uses, applications, and
24 harms of digital content forgeries.

1 (B) MISSION.—The mission of the Bureau
2 established under this paragraph shall be to as-
3 sist the Commission in exercising the Commis-
4 sion’s authority under this Act and under other
5 Federal laws addressing privacy, data security,
6 and related issues.

7 (C) TIMELINE.—Such Bureau shall be es-
8 tablished, staffed, and fully operational within 2
9 years of enactment of this Act.

10 (2) TREATMENT AS VIOLATION OF RULE.—A
11 violation of this Act or a regulation promulgated
12 under this Act shall be treated as a violation of a
13 rule defining an unfair or deceptive act or practice
14 prescribed under section 18(a)(1)(B) of the Federal
15 Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

16 (3) POWERS OF COMMISSION.—

17 (A) IN GENERAL.—Except as provided in
18 subparagraph (C), the Commission shall enforce
19 this Act and the regulations promulgated under
20 this Act in the same manner, by the same
21 means, and with the same jurisdiction, powers,
22 and duties as though all applicable terms and
23 provisions of the Federal Trade Commission
24 Act (15 U.S.C. 41 et seq.) were incorporated
25 into and made a part of this Act.

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

7 (C) INDEPENDENT LITIGATION AUTHOR-
8 ITY.—The Commission may commence, defend,
9 or intervene in, and supervise the litigation of
10 any civil action under this subsection (including
11 an action to collect a civil penalty) and any ap-
12 peal of such action in its own name by any of
13 its attorneys designated by it for such purpose.
14 The Commission shall notify the Attorney Gen-
15 eral of any such action and may consult with
16 the Attorney General with respect to any such
17 action or request the Attorney General on be-
18 half of the Commission to commence, defend, or
19 intervene in any such action.

20 (4) DATA PRIVACY AND SECURITY RELIEF
21 FUND.—

22 (A) ESTABLISHMENT OF RELIEF FUND.—
23 There is established in the Treasury of the
24 United States a separate fund to be known as
25 the “Data Privacy and Security Relief Fund”

1 (referred to in this paragraph as the “Relief
2 Fund”).

3 (B) DEPOSITS.—

4 (i) DEPOSITS FROM THE COMMIS-
5 SION.—The Commission shall deposit into
6 the Relief Fund the amount of any civil
7 penalty obtained against any covered entity
8 in any judicial or administrative action the
9 Commission commences to enforce this Act
10 or a regulation promulgated under this
11 Act.

12 (ii) DEPOSITS FROM THE ATTORNEY
13 GENERAL.—The Attorney General of the
14 United States shall deposit into the Relief
15 Fund the amount of any civil penalty ob-
16 tained against any covered entity in any
17 judicial or administrative action the Attor-
18 ney General commences on behalf of the
19 Commission to enforce this Act or a regu-
20 lation promulgated under this Act.

21 (C) USE OF FUND AMOUNTS.—Notwith-
22 standing section 3302 of title 31, United States
23 Code, amounts in the Relief Fund shall be
24 available to the Commission, without fiscal year
25 limitation, to provide redress, payments or com-

1 pensation, or other monetary relief to individ-
2 uals affected by an act or practice for which
3 civil penalties have been obtained under this
4 Act. To the extent that individuals cannot be lo-
5 cated or such redress, payments or compensa-
6 tion, or other monetary relief are otherwise not
7 practicable, the Commission may use such
8 funds for the purpose of consumer or business
9 education relating to data privacy and security
10 or for the purpose of engaging in technological
11 research that the Commission considers nec-
12 essary to enforce this Act.

13 (D) AMOUNTS NOT SUBJECT TO APPOR-
14 TIONMENT.—Notwithstanding any other provi-
15 sion of law, amounts in the Relief Fund shall
16 not be subject to apportionment for purposes of
17 chapter 15 of title 31, United States Code, or
18 under any other authority.

19 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-
20 ERAL.—

21 (1) CIVIL ACTION.—In any case in which the
22 attorney general of a State or a consumer protection
23 officer of a State has reason to believe that an inter-
24 est of the residents of that State has been or is ad-
25 versely affected by the engagement of any covered

1 entity in an act or practice that violates this Act or
2 a regulation promulgated under this Act, the attor-
3 ney general of the State, or a consumer protection
4 officer of the State acting on behalf of the State, as
5 *parens patriae*, may bring a civil action on behalf of
6 the residents of the State in an appropriate district
7 court of the United States to—

8 (A) enjoin that act or practice;

9 (B) enforce compliance with this Act or the
10 regulation;

11 (C) obtain damages, civil penalties, restitu-
12 tion, or other compensation on behalf of the
13 residents of the State; or

14 (D) obtain such other relief as the court
15 may consider to be appropriate.

16 (2) NOTICE TO THE COMMISSION AND RIGHTS
17 OF THE COMMISSION.—Except where not feasible,
18 the State shall notify the Commission in writing
19 prior to initiating a civil action under paragraph (1).
20 Such notice shall include a copy of the complaint to
21 be filed to initiate such action. If prior notice is not
22 practicable, the State shall provide a copy of the
23 complaint to the Commission immediately upon in-
24 stituting the action. Upon receiving such notice, the

1 Commission may intervene in such action and, upon
2 intervening—

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

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

7 (3) PRESERVATION OF STATE POWERS.—No
8 provision of this section shall be construed as alter-
9 ing, limiting, or affecting the authority of a State at-
10 torney general or a consumer protection officer of a
11 State to—

12 (A) bring an action or other regulatory
13 proceeding arising solely under the law in effect
14 in that State; or

15 (B) exercise the powers conferred on the
16 attorney general or on a consumer protection
17 officer of a State by the laws of the State, in-
18 cluding the ability to conduct investigations, to
19 administer oaths or affirmations, or to compel
20 the attendance of witnesses or the production of
21 documentary or other evidence.

22 (4) VENUE; SERVICE OF PROCESS.—

23 (A) VENUE.—Any action brought under
24 paragraph (1) may be brought in the district
25 court of the United States that meets applicable

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

3 (B) SERVICE OF PROCESS.—In an action
4 brought under paragraph (1), process may be
5 served in any district in which the defendant—

6 (i) is an inhabitant; or

7 (ii) may be found.

8 (c) ENFORCEMENT BY INDIVIDUALS.—

9 (1) IN GENERAL.—Any individual alleging a
10 violation of this Act or a regulation promulgated
11 under this Act may bring a civil action in any court
12 of competent jurisdiction, State or Federal.

13 (2) RELIEF.—In a civil action brought under
14 paragraph (1) in which the plaintiff prevails, the
15 court may award—

16 (A) an amount not less than \$100 and not
17 greater than \$1,000 per violation per day or ac-
18 tual damages, whichever is greater;

19 (B) punitive damages;

20 (C) reasonable attorney's fees and litiga-
21 tion costs; and

22 (D) any other relief, including equitable or
23 declaratory relief, that the court determines ap-
24 propriate.

1 (3) INJURY IN FACT.—A violation of this Act or
2 a regulation promulgated under this Act with re-
3 spect to the covered data of an individual constitutes
4 a concrete and particularized injury in fact to that
5 individual.

6 (d) INVALIDITY OF PRE-DISPUTE ARBITRATION
7 AGREEMENTS AND PRE-DISPUTE JOINT ACTION WAIV-
8 ERS.—

9 (1) IN GENERAL.—Notwithstanding any other
10 provision of law, no pre-dispute arbitration agree-
11 ment or pre-dispute joint action waiver shall be valid
12 or enforceable with respect to a privacy or data secu-
13 rity dispute arising under this Act.

14 (2) APPLICABILITY.—Any determination as to
15 whether or how this subsection applies to any pri-
16 vacy or data security dispute shall be made by a
17 court, rather than an arbitrator, without regard to
18 whether such agreement purports to delegate such
19 determination to an arbitrator.

20 (3) DEFINITIONS.—For purposes of this sub-
21 section:

22 (A) The term “pre-dispute arbitration
23 agreement” means any agreement to arbitrate a
24 dispute that has not arisen at the time of the
25 making of the agreement.

1 (B) The term “pre-dispute joint-action
2 waiver” means an agreement, whether or not
3 part of a pre-dispute arbitration agreement,
4 that would prohibit, or waive the right of, one
5 of the parties to the agreement to participate in
6 a joint, class, or collective action in a judicial,
7 arbitral, administrative, or other forum, con-
8 cerning a dispute that has not yet arisen at the
9 time of the making of the agreement.

10 (C) The term “privacy or data security dis-
11 pute” means any claim relating to an alleged
12 violation of this Act, or a regulation promul-
13 gated under this Act, and between an individual
14 and a covered entity.

15 **SEC. 302. RELATIONSHIP TO FEDERAL AND STATE LAWS.**

16 (a) FEDERAL LAW PRESERVATION.—Nothing in this
17 Act or a regulation promulgated under this Act shall be
18 construed to limit—

19 (1) the authority of the Commission, or any
20 other Executive agency, under any other provision of
21 law; or

22 (2) any other provision of Federal law unless as
23 specifically authorized by this Act.

24 (b) STATE LAW PRESERVATION.—Nothing in this
25 Act shall be construed to preempt, displace, or supplant

1 the following State laws, rules, regulations, or require-
2 ments:

3 (1) Consumer protection laws of general appli-
4 cability such as laws regulating deceptive, unfair, or
5 unconscionable practices.

6 (2) Civil rights laws.

7 (3) Laws that govern the privacy rights or
8 other protections of employees, employee informa-
9 tion, or students or student information.

10 (4) Laws that address notification requirements
11 in the event of a data breach.

12 (5) Contract or tort law.

13 (6) Criminal laws governing fraud, theft, unau-
14 thorized access to information or unauthorized use
15 of information, malicious behavior, and similar pro-
16 visions, and laws of criminal procedure.

17 (7) Laws specifying remedies or a cause of ac-
18 tion to individuals.

19 (8) Public safety or sector specific laws unre-
20 lated to privacy or security.

21 (c) PREEMPTION OF DIRECTLY CONFLICTING STATE
22 LAWS.—Except as provided in subsections (b) and (d),
23 this Act shall supersede any State law to the extent such
24 law directly conflicts with the provisions of this Act, or
25 a standard, rule, or regulation promulgated under this

1 Act, and then only to the extent of such direct conflict.
2 Any State law, rule, or regulation shall not be considered
3 in direct conflict if it affords a greater level of protection
4 to individuals protected under this Act.

5 (d) PRESERVATION OF COMMON LAW OR STATUTORY
6 CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this
7 Act, nor any amendment, standard, rule, requirement, as-
8 sessment, law or regulation promulgated under this Act,
9 shall be construed to preempt, displace, or supplant any
10 Federal or State common law rights or remedies, or any
11 statute creating a remedy for civil relief, including any
12 cause of action for personal injury, wrongful death, prop-
13 erty damage, or other financial, physical, reputational, or
14 psychological injury based in negligence, strict liability,
15 products liability, failure to warn, an objectively offensive
16 intrusion into the private affairs or concerns of the indi-
17 vidual, or any other legal theory of liability under any Fed-
18 eral or State common law, or any State statutory law.

19 **SEC. 303. SEVERABILITY.**

20 If any provision of this Act, or the application thereof
21 to any person or circumstance, is held invalid, the remain-
22 der of this Act and the application of such provision to
23 other persons not similarly situated or to other cir-
24 cumstances shall not be affected by the invalidation.

1 **SEC. 304. AUTHORIZATION OF APPROPRIATIONS.**

2 There are authorized to be appropriated to the Com-
3 mission such sums as may be necessary to carry out this
4 Act.