

**AMENDMENT TO THE AMENDMENT IN THE
NATURE OF A SUBSTITUTE FOR H.R. 2668
OFFERED BY M . _____**

Before section 1 of the bill, insert the following:

1 **DIVISION A—CONSUMER**
2 **PROTECTION AND RECOVERY**

In section 1, strike “This Act” and insert “This division”.

At the end of the bill, insert the following:

3 **DIVISION B—ONLINE PRIVACY**

4 **SEC. 11. SHORT TITLE; TABLE OF CONTENTS.**

5 (a) **SHORT TITLE.**—This division may be cited as the
6 “Online Privacy Act of 2021”.

7 (b) **TABLE OF CONTENTS.**—The table of contents for
8 this division is as follows:

- Sec. 11. Short title; table of contents.
- Sec. 12. Definitions.
- Sec. 13. Prohibition on waivers.
- Sec. 14. Effective date.
- Sec. 15. Journalism protection.
- Sec. 16. Small business compliance ramp.
- Sec. 17. Criminal prohibition on disclosing personal information.
- Sec. 18. Limitation on disclosing nonredacted government records.

TITLE I—INDIVIDUAL RIGHTS

- Sec. 101. Right of access.
- Sec. 102. Right of correction.
- Sec. 103. Right of deletion.
- Sec. 104. Right of portability.

- Sec. 105. Right to human review of automated decisions.
- Sec. 106. Right to individual autonomy.
- Sec. 107. Right to be informed.
- Sec. 108. Right to impermanence.
- Sec. 109. Exemptions, exceptions, fees, timelines, and rules of construction for rights under this title.

TITLE II—REQUIREMENTS FOR COVERED ENTITIES, SERVICE PROVIDERS, AND THIRD PARTIES

- Sec. 201. Minimization and articulated basis for collection, processing, and maintenance.
- Sec. 202. Minimization and records of access by employees and contractors.
- Sec. 203. Prohibition on the collection or maintenance of personal information.
- Sec. 204. Prohibitions on the disclosure of personal information.
- Sec. 205. Disclosure to entities not subject to United States jurisdiction or not compliant with this Act.
- Sec. 206. Prohibition on reidentification.
- Sec. 207. Restrictions on collection, processing, and disclosure of contents of communications.
- Sec. 208. Prohibition on discriminatory processing.
- Sec. 209. Restrictions on genetic information.
- Sec. 210. Requirements for notice and consent processes and privacy policies.
- Sec. 211. Prohibition on deceptive notice and consent processes and privacy policies.
- Sec. 212. Notice and consent required.
- Sec. 213. Privacy policy.
- Sec. 214. Information security requirements.
- Sec. 215. Notification of data breach or data sharing abuse.

TITLE III—UNITED STATES DIGITAL PRIVACY AGENCY

- Sec. 301. Establishment.
- Sec. 302. Executive and administrative powers.
- Sec. 303. Rulemaking authority.
- Sec. 304. Personnel.
- Sec. 305. Complaints of individuals.
- Sec. 306. User advisory board.
- Sec. 307. Academic and research advisory board.
- Sec. 308. Small business and investor advisory board.
- Sec. 309. Consultation.
- Sec. 310. Reports.
- Sec. 311. Grants for developing open-source machine learning training data.
- Sec. 312. Annual audits.
- Sec. 313. Inspector General.
- Sec. 314. Authorization of appropriations.

TITLE IV—ENFORCEMENT

- Sec. 401. Definitions.
- Sec. 402. Investigations and administrative discovery.
- Sec. 403. Hearings and adjudication proceedings.
- Sec. 404. Litigation authority.
- Sec. 405. Coordination with other Federal agencies.
- Sec. 406. Enforcement by States.
- Sec. 407. Private rights of action.

- Sec. 408. Relief available.
- Sec. 409. Referral for criminal proceedings.
- Sec. 410. Whistleblower enforcement.

TITLE V—RELATION TO OTHER LAW

- Sec. 501. Relation to other Federal law.
- Sec. 502. Severability.

1 **SEC. 12. DEFINITIONS.**

2 In this division:

3 (1) AGENCY.—The term “Agency” means the
4 United States Digital Privacy Agency established by
5 section 301.

6 (2) BEHAVIORAL PERSONALIZATION.—

7 (A) IN GENERAL.—The term “behavioral
8 personalization” means the processing of an in-
9 dividual’s personal information, using an algo-
10 rithm, model, or other means built using that
11 individual’s personal information collected over
12 a period of time, or an aggregate of the per-
13 sonal information of one or more similarly situ-
14 ated individuals and designed to—

15 (i) alter, influence, guide, or predict
16 an individual’s behavior;

17 (ii) tailor or personalize a product or
18 service; or

19 (iii) filter, sort, limit, promote, display
20 or otherwise differentiate between specific
21 content or categories of content that would
22 otherwise be accessible to the individual.

1 (B) EXCLUSIONS.—The term “behavioral
2 personalization” does not include the use of his-
3 torical personal information to merely prevent
4 the display of or provide additional information
5 about previously accessed content.

6 (3) COLLECT.—The term “collect” includes,
7 with respect to personal information or contents of
8 communication, obtaining such information in any
9 manner, except when solely transmitting, routing,
10 providing intermediate storage for, or providing con-
11 nections for personal information through a system
12 or network.

13 (4) CONTENTS.—The term “contents”, when
14 used with respect to communication, has the mean-
15 ing given such term in section 2510 of title 18,
16 United States Code.

17 (5) COVERED ENTITY.—

18 (A) IN GENERAL.—The term “covered en-
19 tity” means a person who—

20 (i) intentionally collects, processes, or
21 maintains personal information; and

22 (ii) sends or receives such personal in-
23 formation over the internet or a similar
24 communications network.

1 (B) EXCLUSION.—The term “covered enti-
2 ty” does not include a natural person, except to
3 the extent such person is engaged in a commer-
4 cial activity that is more than de minimis.

5 (6) DATA BREACH.—The term “data breach”
6 means unauthorized access to or acquisition of per-
7 sonal information or contents of communications
8 maintained by such covered entity.

9 (7) DATA SHARING ABUSE.—The term “data
10 sharing abuse” means processing, by a third party,
11 of personal information or contents of communica-
12 tions disclosed by a covered entity to the third party,
13 for any purpose other than—

14 (A) a purpose specified by the covered en-
15 tity to the third party at the time of disclosure;
16 or

17 (B) a purpose to which the individual to
18 whom the information relates has consented.

19 (8) DE-Identified.—

20 (A) IN GENERAL.—The term “de-identi-
21 fied” means information that cannot reasonably
22 identify, relate to, describe, reference, be capa-
23 ble of being associated with, or be linked, di-
24 rectly or indirectly, to a particular individual or

1 device, provided that a business that uses de-
2 identified information—

3 (i) has de-identified the personal in-
4 formation using best practices for the
5 types of data the information contains;

6 (ii) has implemented technical safe-
7 guards that prohibit re-identification of the
8 individual with whom the information was
9 linked;

10 (iii) has implemented business proc-
11 esses that specifically prohibit re-identifica-
12 tion of the information;

13 (iv) has implemented business proc-
14 esses to prevent inadvertent release of de-
15 identified information; and

16 (v) makes no attempt to re-identify
17 the information.

18 (B) The Director may determine that a
19 methodology of de-identifying personal informa-
20 tion is insufficient for the purposes of this defi-
21 nition.

22 (9) DIRECTOR.—The term “Director” means
23 the Director of the Agency.

24 (10) DISCLOSE.—The term “disclose” means,
25 with respect to personal information or contents of

1 communication, to sell, release, transfer, share, dis-
2 seminate, make available, or otherwise cause to be
3 communicated such information to a third party.

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

7 (12) MAINTAIN.—The term “maintain” means,
8 with respect to personal information or contents of
9 communication, to store, secure, or otherwise cause
10 the retaining of such information, or taking actions
11 necessary for such purposes.

12 (13) PERSONAL INFORMATION.—

13 (A) IN GENERAL.—The term “personal in-
14 formation” means any information maintained
15 by a covered entity that is linked or reasonably
16 linkable to a specific individual or a specific de-
17 vice, including de-identified personal informa-
18 tion and the means to behavioral personaliza-
19 tion created for or linked to a specific indi-
20 vidual.

21 (B) EXCLUSIONS.—The term “personal in-
22 formation” does not include—

23 (i) publicly available information re-
24 lated to an individual; or

1 (ii) information derived or inferred
2 from personal information, if the derived
3 or inferred information is not linked or
4 reasonably linkable to a specific individual.

5 (14) PRIVACY HARM.—The term “privacy
6 harm” means adverse consequences or potential ad-
7 verse consequences to an individual or society arising
8 from the collection, processing, maintenance, or dis-
9 closure of personal information, including—

10 (A) direct or indirect financial loss or eco-
11 nomic harm;

12 (B) physical harm;

13 (C) psychological harm, including anxiety,
14 embarrassment, fear, and other demonstrable
15 mental trauma;

16 (D) adverse outcomes or decisions with re-
17 spect to the eligibility of an individual for
18 rights, benefits, or privileges in employment (in-
19 cluding hiring, firing, promotion, demotion, and
20 compensation), credit and insurance (including
21 denial of an application or obtaining less favor-
22 able terms), housing, education, professional
23 certification, or the provision of health care and
24 related services;

25 (E) stigmatization or reputational harm;

1 (F) price discrimination;

2 (G) other adverse consequences that affect
3 the private life of an individual, including pri-
4 vate family matters and actions and commu-
5 nications within the home of such individual or
6 a similar physical, online, or digital location
7 where such individual has a reasonable expecta-
8 tion that personal information will not be col-
9 lected, processed, or retained;

10 (H) chilling of free expression or action of
11 an individual, group of individuals, or society
12 generally, due to perceived or actual pervasive
13 and excessive collection, processing, disclosure,
14 or maintenance of personal information by a
15 covered entity;

16 (I) impairing the autonomy of an indi-
17 vidual, group of individuals, or society gen-
18 erally; and

19 (J) other adverse consequences or potential
20 adverse consequences, consistent with the provi-
21 sions of this division, as determined by the Di-
22 rector.

23 (15) PRIVACY PRESERVING COMPUTING.—

24 (A) IN GENERAL.—The term “privacy pre-
25 serving computing” means—

1 (i) the collecting, processing, dis-
2 closing, or maintaining of personal infor-
3 mation that has been encrypted or other-
4 wise rendered unintelligible using a means
5 that cannot be reversed by a covered enti-
6 ty, or a covered entity's service provider,
7 such that—

8 (I) if such personal information
9 could be rendered intelligible through
10 cooperation or sharing of cryp-
11 tographic secrets by multiple persons,
12 the covered entity has both technical
13 safeguards and business processes to
14 prevent such cooperation or sharing;

15 (II) if such personal information
16 is rendered intelligible within a hard-
17 ware processing unit or other means
18 of performing operations on the infor-
19 mation, there are technical safeguards
20 that, during the normal course of op-
21 eration—

22 (aa) prevent rendering per-
23 sonal information intelligible any-
24 where but within the hardware

1 processing unit or other means of
2 performing operations; and

3 (bb) make the exporting or
4 otherwise observing of such intel-
5 ligible information, or the cryp-
6 tographic secret used to protect
7 such information, impossible; and

8 (III) if the result of such proc-
9 essing of the personal information is
10 also personal information, such result
11 must be unintelligible to the covered
12 entity or service provider and pro-
13 tected by privacy preserving com-
14 puting.

15 (B) INSUFFICIENT METHODOLOGIES.—The
16 Director may determine that a methodology of
17 privacy preserving computing is insufficient for
18 the purposes of this definition.

19 (16) PROCESS.—The term “process” means to
20 perform or cause to be performed any operation or
21 set of operations on personal information or contents
22 of communication, whether or not by automated
23 means.

24 (17) PROTECTED CLASS.—The term “protected
25 class” means the actual or perceived race, color, eth-

1 nicity, national origin, religion, sex (including sexual
2 orientation and gender identity), familial status, or
3 disability of an individual or group of individuals.

4 (18) PUBLICLY AVAILABLE INFORMATION.—

5 The term “publicly available information” means—

6 (A) information that is lawfully made
7 available from Federal, State, or local govern-
8 ment records;

9 (B) information about a public individual
10 or official that is made publicly accessible, with-
11 out restrictions on accessibility other than the
12 general authorization to access the services used
13 to make the information accessible;

14 (C) information made publicly accessible
15 by the individual to whom it pertains, without
16 restrictions on accessibility other than the gen-
17 eral authorization to access the services used to
18 make the information accessible, and that such
19 individual has the ability to delete or change
20 without relying on a request under section 102
21 or 103 of this division; and

22 (D) does not include—

23 (i) biometric information collected by
24 a covered entity relating to an individual
25 without the individual’s knowledge;

1 (ii) information used for a purpose
2 that is not compatible with the purpose for
3 which the information is maintained and
4 made available in government records;

5 (iii) information obtained from gov-
6 ernment records for the purpose of selling
7 such information; or

8 (iv) information used to contact or lo-
9 cate a private individual either physically
10 or electronically.

11 (19) REASONABLE MECHANISM.—The term
12 “reasonable mechanism” means, in the case of a
13 mechanism for individuals to exercise a right under
14 title I or interact with a covered entity under title
15 II, that such mechanism—

16 (A) is equivalent in availability and ease of
17 use to that of other mechanisms for commu-
18 nicating or interacting with the covered entity;
19 and

20 (B) includes an online means of exercising
21 such right or engaging in such interaction, if
22 such individuals communicate or interact with
23 such covered entity through an online medium
24 or if such covered entity provides information
25 processing services through a public or widely

1 available application programming interface (or
2 similar mechanism).

3 (20) SELL AND SALE.—

4 (A) IN GENERAL.—The terms “sell” and
5 “sale” means the disclosure of personal infor-
6 mation for monetary consideration by a covered
7 entity to a third party for the purposes of proc-
8 essing, maintaining or disclosing such personal
9 information at the third party’s discretion.

10 (B) EXCLUSIONS.—The terms “sell” and
11 “sale” do not include—

12 (i) the disclosure of personal data to
13 a third party with which the individual has
14 a direct relationship for purposes of pro-
15 viding a product or service requested by
16 the individual or otherwise in a manner
17 that is consistent with an individual’s rea-
18 sonable expectations considering the con-
19 text in which the individual provided the
20 personal information to the covered entity;

21 (ii) the disclosure or transfer of per-
22 sonal information to a subsidiary or an af-
23 filiate of the covered entity; or

24 (iii) the disclosure or transfer of per-
25 sonal information to a third party as an

1 asset that is part of a merger, acquisition,
2 bankruptcy, or other transaction in which
3 the third party assumes control of all or
4 part of the covered entity's assets, unless
5 such assets are limited to personal infor-
6 mation unless personal information makes
7 up the majority of the value of such assets.

8 (21) SERVICE PROVIDER.—

9 (A) IN GENERAL.—The term “service pro-
10 vider” means a covered entity who—

11 (i) processes, discloses, or maintains
12 personal information, where such person
13 does not process, disclose, or maintain the
14 personal information other than in accord-
15 ance with the directions and on behalf of
16 another covered entity;

17 (ii) does not directly collect personal
18 information from or control the mechanism
19 for collecting personal information from an
20 individual;

21 (iii) does not earn revenue from proc-
22 essing, maintaining, or disclosing personal
23 information disclosed to the service pro-
24 vider by a covered entity except by pro-

1 viding contracted services to another cov-
2 ered entity;

3 (iv) does not disclose personal infor-
4 mation to another covered entity unless it
5 was provided by that covered entity or re-
6 sulted from maintaining or processing per-
7 formed on personal information exclusively
8 provide by that covered entity;

9 (v) does not offer services that allow
10 another covered entity to target specific in-
11 dividuals using personal information not
12 provided by that covered entity;

13 (vi) assists a covered entity on behalf
14 of which it processes personal information
15 to comply with title I, with respect to per-
16 sonal information processed or maintained
17 by the service provider on behalf of the
18 covered entity, including providing tools for
19 such covered entities requirements under
20 title I if requested; and

21 (vii) does not link the personal infor-
22 mation provided by another covered entity
23 to personal information from any other
24 source.

1 (B) Any such person, and the personal in-
2 formation they disclose, process, or maintain,
3 shall be treated as a service provider under this
4 division only to the extent that such person
5 complies with the requirements under (A).

6 (22) SIGNIFICANT PRIVACY HARM.—The term
7 “significant privacy harm” means adverse con-
8 sequences to an individual arising from the collec-
9 tion, processing, maintenance, or disclosure of per-
10 sonal information, limited to subparagraph (A), (B),
11 or (D) of paragraph (14).

12 (23) SMALL BUSINESS.—The term “small busi-
13 ness” means a covered entity that—

14 (A) does not earn revenue from the sale of
15 personal information;

16 (B) earns less than half of annual revenues
17 from the processing of personal information for
18 targeted or personalized advertising;

19 (C) has not, at any time during the pre-
20 ceeding 6-month period, maintained personal in-
21 formation of 250,000 or more individuals;

22 (D) has fewer than 200 employees; and

23 (E) received less than \$25,000,000 in
24 gross revenue in the preceding 12-month pe-
25 riod.

1 (24) STATE.—The term “State” means each
2 State of the United States, the District of Columbia,
3 each commonwealth, territory, or possession of the
4 United States, and each federally recognized Indian
5 Tribe.

6 (25) THIRD PARTY.—The term “third party”
7 means, with respect to a covered entity, a person—

8 (A) to whom such covered entity disclosed
9 personal information; and

10 (B) is not—

11 (i) such covered entity;

12 (ii) a subsidiary or corporate affiliate
13 of such covered entity; or

14 (iii) a service provider of such covered
15 entity.

16 **SEC. 13. PROHIBITION ON WAIVERS.**

17 (a) IN GENERAL.—The provisions under this division
18 may not be waived. Any agreement purporting to waive
19 compliance with or modify any provision of this division
20 shall be void as contrary to public policy.

21 (b) PROHIBITION ON PREDISPUTE ARBITRATION
22 AGREEMENTS.—No predispute arbitration agreement
23 shall be valid or enforceable with respect to any claims
24 under this division.

1 **SEC. 14. EFFECTIVE DATE.**

2 (a) IN GENERAL.—This division shall apply begin-
3 ning on the date that is 1 year after the date of the enact-
4 ment of this Act.

5 (b) AUTHORITY TO PROMULGATE REGULATIONS AND
6 TAKE CERTAIN OTHER ACTIONS.—Nothing in subsection
7 (a) affects the authority to take an action expressly re-
8 quired by a provision of this division to be taken before
9 the effective date described in such subsection.

10 **SEC. 15. JOURNALISM PROTECTION.**

11 (a) IN GENERAL.—Covered entities engaged in jour-
12 nalism shall not be subject to the obligations imposed
13 under this division to the extent that those obligations di-
14 rectly infringe on the journalism rather than the business
15 practices of the covered entity, so long as, the covered enti-
16 ty has technical safeguards and business processes that
17 prevent the collection, processing, maintaining, or disclo-
18 sure of such personal information for business practices
19 other than journalism.

20 (b) JOURNALISM.—The term “journalism” includes
21 the collecting, maintaining, processing, and disclosing of
22 personal information about a public individual or official,
23 or that otherwise concerns matters of public interest, for
24 dissemination to the public.

1 **SEC. 16. SMALL BUSINESS COMPLIANCE RAMP.**

2 Upon losing its status as a small business, a covered
3 entity shall have nine months to comply with provisions
4 of this division that a small business is exempt from com-
5 plying with.

6 **SEC. 17. CRIMINAL PROHIBITION ON DISCLOSING PER-**
7 **SONAL INFORMATION.**

8 Chapter 41 of title 18, United States Code, is amend-
9 ed by adding at the end the following:

10 **“§ 881. Disclosure of personal information with the**
11 **intent to cause harm**

12 “Whoever uses a channel of interstate or foreign com-
13 merce to knowingly disclose an individual’s personal infor-
14 mation—

15 “(1) with the intent to threaten, intimidate, or
16 harass any person, incite or facilitate the commis-
17 sion of a crime of violence against any person, or
18 place any person in reasonable fear of death or seri-
19 ous bodily injury; or

20 “(2) with the intent that the information will be
21 used to threaten, intimidate, or harass any person,
22 incite or facilitate the commission of a crime of vio-
23 lence against any person, or place any person in rea-
24 sonable fear of death or serious bodily injury,

25 shall be fined under this title or imprisoned not more than
26 5 years, or both.”.

1 **SEC. 18. LIMITATION ON DISCLOSING NONREDACTED GOV-**
2 **ERNMENT RECORDS.**

3 (a) IN GENERAL.—A Federal or State government
4 entity may not use a channel of interstate commerce to
5 disclose the personal information of an individual in a gov-
6 ernment record without an agreement prohibiting the re-
7 cipient of such information from selling the information
8 without the express consent of the individual for each dis-
9 closure.

10 (b) EXCEPTION.—Notwithstanding subsection (a),
11 nothing in this section shall prohibit the disclosure of per-
12 sonal information using a channel of interstate commerce
13 to another government entity without consent of the indi-
14 vidual.

15 **TITLE I—INDIVIDUAL RIGHTS**

16 **SEC. 101. RIGHT OF ACCESS.**

17 (a) IN GENERAL.—A covered entity shall make avail-
18 able a reasonable mechanism by which an individual may
19 access—

20 (1) the categories of personal information and
21 contents of communications of such individual that
22 is maintained by such covered entity, including, in
23 the case of personal information that such covered
24 entity did not collect from such individual, how and
25 from whom such covered entity obtained such per-
26 sonal information;

1 (2) a list of the third parties, subsidiaries, and
2 corporate affiliates, to which such covered entity has
3 disclosed and from which such covered entity has, at
4 any time on or after the effective date specified in
5 section 4(a), obtained the personal information of
6 such individual;

7 (3) a concise and clear description of the busi-
8 ness or commercial purposes of such covered enti-
9 ty—

10 (A) for collecting, processing, or maintain-
11 ing the personal information of such individual;
12 and

13 (B) for disclosing to a third party the per-
14 sonal information of such individual; and

15 (4) a list of automated decision-making proc-
16 esses that an individual has a right to request
17 human review of under section 105 with a concise
18 and clear description of the implications and in-
19 tended effects of such process.

20 (b) EXCEPTION FOR PUBLICLY ACCESSIBLY INFOR-
21 MATION.—A covered entity that makes available informa-
22 tion required in subsection (a) shall be considered in com-
23 pliance with such requirements if the covered entity pro-
24 vides an individual instructions on how to access a public

1 posting of such information, including in a privacy policy,
2 if the instructions are easy and do not require payment.

3 (c) **SMALL BUSINESSES EXCLUDED.**—Subsection
4 (a)(3) does not apply to a small business.

5 **SEC. 102. RIGHT OF CORRECTION.**

6 (a) **DISPUTE BY INDIVIDUAL.**—A covered entity shall
7 make available a reasonable mechanism by which an indi-
8 vidual may dispute the accuracy or completeness of per-
9 sonal information linked to such individual that is main-
10 tained by such covered entity if such information is proc-
11 essed in any way, by such covered entity, a third party
12 of such covered entity, or a service provider of such cov-
13 ered entity that may increase reasonably foreseeable sig-
14 nificant privacy harms.

15 (b) **CORRECTION BY COVERED ENTITY.**—A covered
16 entity receiving a dispute under subsection (a) shall—

17 (1) correct or complete (as the case may be) the
18 disputed information and notify such individual that
19 the correction or completion has been made; or

20 (2) notify such individual that—

21 (A) the disputed information is correct or
22 complete;

23 (B) such covered entity lacks sufficient in-
24 formation to correct or complete the disputed
25 information; or

1 (C) such covered entity is denying the re-
2 quest for correction or completion in reliance on
3 an exemption or exception provided by section
4 109(g) (with the notification containing an
5 identification of the specific exemption or excep-
6 tion relied upon).

7 (c) **SMALL BUSINESSES EXCLUDED.**—This section
8 does not apply to a small business.

9 **SEC. 103. RIGHT OF DELETION.**

10 (a) **REQUEST BY INDIVIDUAL.**—A covered entity
11 shall make available a reasonable mechanism by which an
12 individual may request the deletion of personal informa-
13 tion and contents of communications of such individual
14 maintained by such covered entity, including any such in-
15 formation that such covered entity acquired from a third
16 party or inferred from other information maintained by
17 such covered entity.

18 (b) **DELETION BY COVERED ENTITY.**—A covered en-
19 tity receiving a request for deletion under subsection (a)
20 shall—

21 (1) delete such information and notify such in-
22 dividual that such information has been deleted; or

23 (2) notify such individual that such covered en-
24 tity is denying the request for deletion in reliance on
25 an exemption or exception provided by section

1 109(g) (with the notification containing an identi-
2 fication of the specific exemption or exception relied
3 upon).

4 **SEC. 104. RIGHT OF PORTABILITY.**

5 (a) DETERMINATION OF PORTABLE CATEGORIES.—

6 (1) ANNUAL DETERMINATION.—Not less fre-
7 quently than once per year, the Director shall—

8 (A) establish categories of products and
9 services offered by covered entities, based on
10 similarities in the products and services;

11 (B) determine which categories established
12 under subparagraph (A) are portable categories;
13 and

14 (C) publish in the Federal Register a list
15 of portable categories determined under sub-
16 paragraph (B).

17 (2) OPPORTUNITY FOR PUBLIC COMMENT.—Be-
18 fore publishing the final list under paragraph (1)(C),
19 the Director shall—

20 (A) publish a draft of such list in the Fed-
21 eral Register; and

22 (B) provide for an opportunity for public
23 comment on such draft list.

24 (b) EXERCISE OF RIGHT.—

1 (1) IN GENERAL.—A covered entity that offers
2 a product or service in a portable category shall
3 make available to an individual whose personal infor-
4 mation or contents of communications such entity
5 maintains a reasonable mechanism by which such in-
6 dividual may—

7 (A) download, in a format that is struc-
8 tured, commonly used, and machine-readable—

9 (i) any personal information of such
10 individual that such individual has pro-
11 vided to such covered entity, with the op-
12 tion to download such information by cat-
13 egory that is accessible under section 101
14 of this division; and

15 (ii) any contents of communications;
16 and

17 (B) using a real-time application program-
18 ming interface, or similar mechanism, transmit
19 all personal information and contents of com-
20 munications of or related to such individual
21 (whether or not provided to such covered entity
22 by such individual) from such covered entity to
23 another covered entity in accordance with sub-
24 section (c).

1 (2) REQUIREMENTS FOR APPLICATION PRO-
2 GRAMMING INTERFACE.—The application program-
3 ming interface, or similar mechanism, required by
4 paragraph (1)(B) shall—

5 (A) be publicly documented;

6 (B) allow the option of data to be obtained
7 by category that is accessible under section 101;

8 (C) include a publicly available, fully func-
9 tional test version for development purposes;
10 and

11 (D) be of similar quality to mechanisms
12 used internally by the covered entity.

13 (c) REQUIREMENTS FOR ACCESS TO APPLICATION
14 PROGRAMMING INTERFACE.—

15 (1) ACCESS.—A covered entity shall provide ac-
16 cess to the application programming interface or
17 similar mechanism required by subsection (b)(1)(B)
18 upon the request of another covered entity if the re-
19 questing covered entity has self-certified, using the
20 procedures established by the Director under para-
21 graph (3)(A), that such requesting covered entity—

22 (A) is a covered entity;

23 (B) can have personal information dis-
24 closed to it under section 205 of this division;

1 (C) is, at the time of the self-certification,
2 in compliance with all requirements of this divi-
3 sion (including provisions a small business is
4 otherwise exempt from complying with);

5 (D) will continue to comply with all re-
6 quirements of this division; and

7 (E) will only use such application program-
8 ming interface or similar mechanism at the ex-
9 press request of an individual.

10 (2) DENIAL OF ACCESS.—

11 (A) IN GENERAL.—A covered entity may
12 deny access to the application programming
13 interface or similar mechanism required by sub-
14 section (b)(1)(B) if such covered entity has an
15 objective, reasonable belief that the requesting
16 covered entity has failed to meet the require-
17 ments for self-certification under paragraph (1).

18 (B) REVIEW.—In accordance with the pro-
19 cedures established under paragraph (3)(B), a
20 covered entity the request of which is denied
21 under subparagraph (A) may petition the Di-
22 rector for review of the denial. If the Director
23 finds that such denial is unreasonable, the Di-
24 rector may impose a penalty, to be established

1 in such procedures, on the covered entity that
2 denied the request.

3 (3) CERTIFICATION AND REVIEW PROCE-
4 DURES.—The Director shall establish—

5 (A) procedures for a covered entity to self-
6 certify under paragraph (1); and

7 (B) procedures for the review of petitions
8 under paragraph (2)(B), including penalties for
9 unreasonable denials.

10 (d) SMALL BUSINESSES EXCLUDED.—This section
11 does not apply to a small business.

12 (e) DEFINITIONS.—In this section:

13 (1) PORTABLE CATEGORY.—The term “portable
14 category” means a category of products and services
15 established by the Director under subsection
16 (a)(1)(A)—

17 (A) for which the sum obtained by adding
18 the number of users or estimated users of each
19 product or service in such category is greater
20 than 10,000,000; and

21 (B) that—

22 (i) has an estimated Herfindahl-
23 Hirschman Index of 2,000 or greater;

1 (ii) the total number of covered enti-
2 ties offering products and services in such
3 category is 3 or less; or

4 (iii) the Director otherwise determines
5 that a category would benefit from encour-
6 aging increased competition.

7 (2) **USERS.**—The term “users” means, with re-
8 spect to a product or service, the monthly active
9 users, subscribers, or customers (or a reasonable
10 proxy or substitute therefor determined by the Di-
11 rector) of such product or service.

12 **SEC. 105. RIGHT TO HUMAN REVIEW OF AUTOMATED DECI-**
13 **SIONS.**

14 For any decision by a covered entity based solely on
15 automated processing of personal information of an indi-
16 vidual, if such processing increases reasonably foreseeable
17 significant privacy harms for such individual, such covered
18 entity shall—

19 (1) inform such individual of what personal in-
20 formation is or may be used for such decision;

21 (2) make available a reasonable mechanism by
22 which such individual may request human review of
23 such decision; and

1 (3) if such individual requests such a review,
2 conduct such review within a reasonable amount of
3 time after such request.

4 **SEC. 106. RIGHT TO INDIVIDUAL AUTONOMY.**

5 (a) IN GENERAL.—A covered entity shall not collect,
6 process, maintain, or disclose an individual’s personal in-
7 formation to:

8 (1) create, improve upon, or maintain;

9 (2) process with; or

10 (3) otherwise link an individual with;

11 an algorithm, model, or other means designed for behav-
12 ioral personalization, without the affirmative express con-
13 sent of that individual.

14 (b) CONSENT.—A covered entity must obtain express
15 affirmative consent from an individual before it may pro-
16 vide a behaviorally personalized version of a product or
17 service. Where consent is denied, a covered entity must
18 provide the product or service without behavioral personal-
19 ization.

20 (c) EXCEPTIONS TO PROVIDING PRODUCT OR SERV-
21 ICE.—

22 (1) Where the offering of a substantially similar
23 product or service without behavioral personalization
24 is infeasible, a covered entity shall provide, to the
25 greatest extent feasible, a core aspect or part of the

1 product or service that can be offered without behav-
2 ioral personalization.

3 (2) Where no core aspect or part of the product
4 or service can function in a substantially similar
5 function without behavioral personalization, a cov-
6 ered entity may deny providing an individual use of
7 such product or service if such individual does not
8 consent to behavioral personalization as required in
9 subsection (a).

10 (d) EXCEPTION TO BEHAVIORAL PROCESSING.—Not-
11 withstanding subsections (a) and (b), a covered entity may
12 create or process using behavioral personalization algo-
13 rithms, models, or other mechanisms for the purpose of
14 increasing the usability of the product or service provided
15 by a covered entity that—

16 (1) are built using aggregated personal infor-
17 mation that is representative of all the personal in-
18 formation the covered entity maintains; and

19 (2) have an output that is both uniform across
20 the individuals that use the product or service and
21 independent of a specific individual’s inherent or be-
22 havioral characteristics.

23 (e) USABILITY.—The term “usability” as used in
24 subsection (d) does not include optimizations or other al-
25 terations to the product or service that are made with the

1 primary purpose of increasing the amount of time an indi-
2 vidual engages with or uses the product or service, unless
3 such increase benefits the individual

4 (f) **SMALL BUSINESSES EXCLUDED.**—This section
5 does not apply to a small business.

6 **SEC. 107. RIGHT TO BE INFORMED.**

7 A covered entity that collects personal information of
8 an individual with whom such covered entity does not have
9 an existing relationship (as of the time of the collection),
10 if such personal information includes contact information,
11 shall notify such individual within 30 days, in writing if
12 possible and at no charge to the individual, that such cov-
13 ered entity has collected the personal information of such
14 individual.

15 **SEC. 108. RIGHT TO IMPERMANENCE.**

16 (a) **LIMITATION ON MAINTENANCE OF PERSONAL IN-**
17 **FORMATION.**—A covered entity shall not maintain per-
18 sonal information for more time than expressly consented
19 to by an individual whose personal information is being
20 maintained.

21 (b) **CONSENT.**—A covered entity must obtain express
22 affirmative consent from an individual before maintaining
23 the personal information of such individual for any dura-
24 tion. Such consent may be obtained for categories of per-
25 sonal information and shall give an individual options to

1 affirmatively choose granting a covered entity consent for
2 various durations, at least including—

3 (1) for no longer than needed to complete the
4 specific request or transaction (including a reason-
5 able estimate of such duration by the covered enti-
6 ty);

7 (2) until consent is revoked; and

8 (3) one or more additional durations based on
9 reasonable expectations and norms for the mainte-
10 nance of the category of personal information being
11 maintained.

12 (c) EXCEPTION FOR IMPLIED CONSENT.—Where the
13 long-term maintenance of personal information is, on its
14 face, obvious and a core feature of the product or service
15 at the request of the individual, and the personal informa-
16 tion is maintained only to provide such product or service,
17 subsections (a) and (b) shall not apply.

18 **SEC. 109. EXEMPTIONS, EXCEPTIONS, FEES, TIMELINES,**
19 **AND RULES OF CONSTRUCTION FOR RIGHTS**
20 **UNDER THIS TITLE.**

21 (a) EXEMPTIONS FOR PERSONAL INFORMATION FOR
22 PARTICULAR PURPOSES.—

23 (1) IN GENERAL.—This title does not apply
24 with respect to personal information that is col-
25 lected, processed, maintained, or disclosed for any of

1 the following purposes (or a combination of such
2 purposes), where a covered entity has technical safe-
3 guards and business processes that limit the collec-
4 tion, processing, maintaining, or disclosure of such
5 personal information to the following purposes:

6 (A) Detecting, responding to, or preventing
7 security incidents or threats.

8 (B) Protecting against malicious, decep-
9 tive, fraudulent, or illegal activity.

10 (C) Complying with specific law enforce-
11 ment requests or court orders.

12 (D) Protecting a legally recognized privi-
13 lege or other legal right.

14 (E) Protecting public safety.

15 (F) Collection, processing, or maintenance
16 by an employer pursuant to an employer-em-
17 ployee relationship of records about employees
18 or employment status, except—

19 (i) where the information would not
20 be reasonably expected to be collected in
21 the context of an employee's regular du-
22 ties; or

23 (ii) was disclosed to the employer by
24 a third party.

1 (G) Preventing prospective abuses of a
2 service by an individual whose account has been
3 previously terminated.

4 (H) Routing a communication through a
5 communications network or resolving the loca-
6 tion of a host or client on a communications
7 network.

8 (I) Providing transparency in advertising
9 or origination of user generated content.

10 (2) REIDENTIFICATION.—Where compliance
11 with this title would require the reidentification of
12 de-identified personal information, and the covered
13 entity does not already maintain the information
14 necessary for such reidentification, the covered enti-
15 ty shall be exempt from such compliance, except for
16 with section 106.

17 (3) DISCLOSURE.—A covered entity relying on
18 an exemption under paragraph (1) with respect to
19 personal information shall disclose in the privacy
20 policy maintained by such entity under section
21 213—

22 (A) the reason for which such information
23 is collected, processed, maintained, or disclosed;
24 and

1 (B) a description of the rights provided by
2 this title that are not available with respect to
3 such personal information by reason of such ex-
4 emption.

5 (b) EXCEPTIONS FOR PARTICULAR REQUESTS.—

6 (1) IN GENERAL.—A covered entity may deny
7 the request of an individual under this title if—

8 (A) such covered entity cannot confirm the
9 identity of such individual;

10 (B) such covered entity determines that
11 granting the request of such individual would
12 create a legitimate risk to the privacy, security,
13 safety, or other rights of another individual;

14 (C) such covered entity determines that
15 granting the request of such individual would
16 create a legitimate risk to free expression; or

17 (D) the personal information requested to
18 be corrected under section 102 or deleted under
19 section 103—

20 (i) is necessary to the completion of a
21 transaction initiated before such request
22 was made or the performance of a contract
23 entered into before such request was made;

1 (ii) was collected specifically for the
2 completion of such transaction or the per-
3 formance of such contract; and

4 (iii) would undermine the integrity of
5 a legally significant transaction.

6 (2) LIMITATIONS ON REQUESTS FOR ADDI-
7 TIONAL INFORMATION TO CONFIRM IDENTITY.—A
8 covered entity may not deny a request of an indi-
9 vidual under paragraph (1)(A) on the basis of the
10 refusal of such individual to provide additional per-
11 sonal information to such covered entity to confirm
12 the identity of such individual—

13 (A) if the identity of such individual can
14 reasonably be confirmed using personal infor-
15 mation of such individual that such covered en-
16 tity (as of the time of the request) already
17 maintains; or

18 (B) if such individual has an existing rela-
19 tionship (as of the time of the request) with
20 such covered entity, such individual has con-
21 firmed the identity of such individual to such
22 covered entity in the same manner as for other
23 transactions of a similar sensitivity.

24 (c) EXEMPTION FOR SERVICE PROVIDERS.—This
25 title does not apply to a service provider.

1 (d) EXEMPTION FOR PRIVACY PRESERVING COM-
2 PUTING.—Except for sections 101, 105, 106, and 109,
3 this title does not apply to personal information secured
4 using privacy preserving computing.

5 (e) TIMELINE FOR COMPLYING WITH A REQUEST.—
6 Without undue delay but not longer than 30 days after
7 the request, a covered that receives a request under this
8 title must—

9 (1) comply with such request; or

10 (2) inform such individual of the reason for de-
11 nying such request, as allowed under subsections (a)
12 or (b) of this section.

13 (f) FEES PROHIBITED.—

14 (1) IN GENERAL.—Except as provided in para-
15 graph (2), a covered entity may not charge a fee to
16 an individual for a request made under this title.

17 (2) UNFOUNDED OR EXCESSIVE REQUESTS.—If
18 a request under this title is unfounded or excessive,
19 a covered entity may charge a reasonable fee that
20 reflects the estimated administrative costs of com-
21 plying with such request.

22 (3) AGENCY NOTICE.—If a covered entity plans
23 to charge fee under paragraph (2), it must notify
24 the Agency at least 7 days before charging such fee.

1 (4) AGENCY REVIEW.—The Director may reject
2 any fee that a covered entity plans to charge for a
3 request made under this title if the Agency finds—

4 (A) such fee to be unreasonable relative to
5 reasonable administrative costs of complying
6 with a request under this title; or

7 (B) such request is not unfounded or ex-
8 cessive.

9 (g) RULES OF CONSTRUCTION.—Nothing in this title
10 shall be construed to require a covered entity to—

11 (1) take an action that would convert informa-
12 tion that is not personal information into personal
13 information;

14 (2) collect or maintain personal information or
15 contents of communication that the covered entity
16 would otherwise not maintain; or

17 (3) maintain personal information or contents
18 of communication longer than the covered entity
19 would otherwise maintain such personal information.

20 (h) REGULATIONS.—The Director shall promulgate
21 regulations to implement this section.

1 **TITLE II—REQUIREMENTS FOR**
2 **COVERED ENTITIES, SERVICE**
3 **PROVIDERS, AND THIRD PAR-**
4 **TIES**

5 **SEC. 201. MINIMIZATION AND ARTICULATED BASIS FOR**
6 **COLLECTION, PROCESSING, AND MAINTENANCE.**
7 **NANCE.**

8 (a) **ARTICULATED BASIS.**—A covered entity shall
9 have a reasonable, articulated basis for the collection,
10 processing, disclosure, and maintenance of personal infor-
11 mation that takes into account the reasonable business
12 needs of the covered entity and minimum amount of per-
13 sonal information necessary for providing the service, bal-
14 anced with the intrusion on the privacy of, potential pri-
15 vacy harms to, and reasonable expectations of individuals
16 to whom the personal information relates.

17 (b) **MINIMIZATION OF COLLECTION, PROCESSING,**
18 **DISCLOSURE, AND MAINTENANCE.**—

19 (1) **COLLECTION.**—A covered entity may not
20 collect more personal information than is reasonably
21 needed to provide a product or service that an indi-
22 vidual has requested.

23 (2) **PROCESSING.**—A covered entity may not
24 process personal information for a purpose other
25 than the purpose for which such information was

1 originally collected from the individual or in the case
2 of a service provider, a purpose other than that
3 which is in accordance with the directions of a cov-
4 ered entity.

5 (3) DISCLOSURE.—A covered entity may not
6 disclose personal information for a purpose other
7 than the purpose for which such information was
8 originally collected from the individual or in the case
9 of a service provider, a purpose other than that
10 which is in accordance with the directions of a cov-
11 ered entity.

12 (4) MAINTENANCE.—A covered entity may not
13 maintain personal information once such information
14 is no longer needed for the purpose for which such
15 information was originally collected from the indi-
16 vidual or in the case of a service provider, a purpose
17 other than that which is in accordance with the di-
18 rections of a covered entity.

19 (c) ANCILLARY COLLECTION, PROCESSING, DISCLO-
20 SURE, AND MAINTENANCE.—Notwithstanding subsection
21 (b), a covered entity may engage in collection, processing,
22 disclosure, or maintenance of personal information beyond
23 limitations under subsection (b) only if such covered entity
24 complies with this subsection.

1 (1) NO NOTICE OR CONSENT REQUIRED.—A
2 covered entity may engage in collection, processing,
3 or maintenance of personal information without ad-
4 ditional notice or consent if the purpose for such col-
5 lection, processing, or maintenance is substantially
6 similar to the type of personal information and pur-
7 pose for which such personal information was origi-
8 nally collected and such ancillary collection, proc-
9 essing, or maintenance will not result in additional
10 or increased privacy harms.

11 (2) NOTICE REQUIRED.—A covered entity shall
12 provide notice of ancillary collection, processing, dis-
13 closure or maintenance of personal information in
14 the case of one, but not more than one, of the fol-
15 lowing:

16 (A) Such ancillary collection, processing,
17 disclosure, or maintenance may result in addi-
18 tional or increased privacy harms (but not in-
19 creased significant privacy harms), and is sub-
20 stantially similar to the purpose for which such
21 personal information was originally collected.

22 (B) The purpose for such ancillary collec-
23 tion, processing, disclosure, or maintenance is
24 not substantially similar to the purpose for
25 which such personal information was originally

1 collected, but will not result in additional or in-
2 creased privacy harms.

3 (C) Such ancillary collection, processing,
4 disclosure, or maintenance may result in addi-
5 tional or increased privacy harms (but not in-
6 creased significant privacy harms) and the pur-
7 pose is not substantially similar to the purpose
8 for which such personal information was origi-
9 nally collected, so long as, the personal informa-
10 tion is secured using privacy preserving com-
11 puting.

12 (3) NOTICE AND CONSENT REQUIRED.—For
13 scenarios not covered under paragraph (1) or (2),
14 and notwithstanding section 212(b)(2) and (3), a
15 covered entity shall provide notice of and obtain con-
16 sent for ancillary collection, processing, disclosure or
17 maintenance of personal information.

18 (d) SUBSTITUTION.—In cases in which personal in-
19 formation can be replaced with artificial personal informa-
20 tion, personal information that has been de-identified, or
21 the random personal information of a one or more individ-
22 uals without substantially reducing the utility of the data
23 or requiring an unreasonable amount of effort, such a re-
24 placement shall take place.

1 **SEC. 202. MINIMIZATION AND RECORDS OF ACCESS BY EM-**
2 **PLOYEES AND CONTRACTORS.**

3 (a) MINIMIZATION.—A covered entity shall restrict
4 access to personal information and contents of commu-
5 nications by the employees or contractors of such covered
6 entity based on an articulated balance between the poten-
7 tial for privacy harm, reasonable expectations of individ-
8 uals to whom the personal information relates, and reason-
9 able business needs.

10 (b) RECORDS OF ACCESS.—

11 (1) IN GENERAL.—A covered entity shall main-
12 tain records identifying each instance in which an
13 employee or a contractor of such covered entity ac-
14 cesses personal information or contents of commu-
15 nications if disclosure of, or a data breach or data
16 sharing abuse involving, such personal information
17 or contents may foreseeably result in increased pri-
18 vacy harms.

19 (2) INFORMATION REQUIRED.—The records re-
20 quired by paragraph (1) shall include the following:

21 (A) A unique identifier for the employee or
22 contractor accessing personal information or
23 contents of communications.

24 (B) The date and time of access.

25 (C) The fields of information accessed.

1 (D) The individuals whose personal infor-
2 mation was accessed or the contents of whose
3 communications were accessed.

4 (3) SMALL BUSINESSES EXCLUDED.—This sub-
5 section does not apply to a small business.

6 **SEC. 203. PROHIBITION ON THE COLLECTION OR MAINTENANCE OF PERSONAL INFORMATION.**

8 A covered entity may not collect or maintain personal
9 information using a channel of interstate commerce unless
10 such covered entity is in compliance with all requirements
11 of this division.

12 **SEC. 204. PROHIBITIONS ON THE DISCLOSURE OF PERSONAL INFORMATION.**

14 (a) CONSENT FOR DISCLOSURE REQUIRED.—

15 (1) IN GENERAL.—A covered entity may not in-
16 tentiously disclose personal information unless the
17 covered entity obtains consent of the individual
18 whose personal information is being disclosed for
19 each category of third party to which such personal
20 information will be disclosed. Such covered entity
21 must also provide such individual with notice of—

22 (A) each category of third party;

23 (B) the personal information to be dis-
24 closed; and

1 (C) a concise and clear description of the
2 business or commercial purpose for such disclo-
3 sure.

4 (2) ADDITIONAL REQUIREMENTS FOR SALE OF
5 PERSONAL INFORMATION.—

6 (A) IN GENERAL.—A covered entity may
7 not intentionally sell personal information un-
8 less the covered entity—

9 (i) obtains the consent required by
10 paragraph (1) for each individual disclo-
11 sure of such person information; and

12 (ii) and provides the individual to
13 whom such personal information relates
14 with the identity of the specific third party
15 to which such personal information will be
16 disclosed.

17 (B) DISCLOSURE SERVICES.—Subpara-
18 graph (A) shall not apply to a covered entity in
19 a case in which an individual is directing the
20 covered entity to disclose the personal informa-
21 tion of such individual for the sole purpose of
22 procuring goods or services, or offers for goods
23 or services, for such individual, if there is a rea-
24 sonable mechanism for the individual to with-
25 draw consent.

1 (3) REQUIREMENT TO INCLUDE ORIGINAL PUR-
2 POSE OF COLLECTION.—A covered entity may not
3 intentionally disclose personal information without
4 including the purpose for which the personal infor-
5 mation was originally collected.

6 (4) EXCEPTION FOR PRIVACY PRESERVING
7 COMPUTING.—Notwithstanding paragraph (1), con-
8 sent is not required for a disclosure (not including
9 sale) of personal information secured using privacy
10 preserving computing.

11 (5) EXCEPTION FOR DE-IDENTIFIED PERSONAL
12 INFORMATION.—Notwithstanding paragraph (1),
13 consent is not required for a disclosure (not includ-
14 ing sale) of de-identified personal information where
15 the disclosed personal information is limited to the
16 narrowest possible scope likely to yield the intended
17 benefit and contractual obligations are in place that
18 prohibit—

19 (A) re-identification of the disclosed per-
20 sonal information; and

21 (B) the processing of additional personal
22 information in combination with the disclosed
23 personal information that would allow for the
24 reidentification of the disclosed personal infor-
25 mation.

1 (b) DISCLOSURE FOR ADVERTISING OR MARKETING
2 PURPOSES.—

3 (1) IN GENERAL.—A covered entity may not in-
4 tentiously disclose for advertising or marketing pur-
5 poses a unique identifier or any other personal infor-
6 mation that would allow the disclosure of such infor-
7 mation to be linked to past or future disclosures of
8 information relating to the same individual or device.

9 (2) TREATMENT OF CERTAIN TYPES OF INFOR-
10 MATION.—A disclosure for advertising or marketing
11 purposes may not be treated as violating subpara-
12 graph (1) by reason of including any or all of the
13 following:

14 (A) Internet Protocol addresses truncated
15 to no more than the first 24 bits for Internet
16 Protocol version 4 and the first 48 bits for
17 Internet Protocol version 6, or for a successor
18 protocol truncated to limit the precision of the
19 identifier to a network address of the internet
20 access provider.

21 (B) Geolocation information truncated to
22 allow no more than the equivalent of two dec-
23 imal degrees of precision at the equator or
24 prime meridian, or an equivalent precision in
25 another geolocation standard.

1 (C) A general description of a device,
2 browser, or operating system, or any combina-
3 tion thereof.

4 (D) An identifier that is unique for each
5 disclosure.

6 **SEC. 205. DISCLOSURE TO ENTITIES NOT SUBJECT TO**
7 **UNITED STATES JURISDICTION OR NOT COM-**
8 **PLIANT WITH THIS ACT.**

9 (a) PROHIBITION.—A covered entity may not inten-
10 tionally disclose personal information to any entity that—

11 (1) is not subject to the jurisdiction of the
12 United States; or

13 (2) is not in compliance with all requirements
14 of this division.

15 (b) EXCEPTION.—Notwithstanding subsection (a), a
16 covered entity may disclose personal information where
17 that personal information is limited to an identifier cre-
18 ated primarily for the purpose of sending or receiving elec-
19 tronic communications and the sole purpose of the disclo-
20 sure is to send or receive an electronic communication at
21 the request of the individual whose personal information
22 is being disclosed.

23 (c) DISCLOSURE SAFE HARBORS.—Notwithstanding
24 subsection (a), a covered entity may disclose personal in-
25 formation to another covered entity (the receiving covered

1 entity) that is not subject to the jurisdiction of the United
2 States if either—

3 (1) the receiving covered entity has entered into
4 an agreement, as described in subsection (e), with
5 the Agency, and—

6 (A) the covered entity has a reasonable be-
7 lief that the receiving covered entity is suffi-
8 ciently solvent to compensate victims or pay
9 fines for violations of this division;

10 (B) a contract between the covered entity
11 and receiving covered entity requires that the
12 receiving covered entity complies with this divi-
13 sion, and the covered entity has reason to be-
14 lieve the receiving covered entity is compliant
15 with this division; and

16 (C) a contract between the covered entity
17 and the receiving covered entity prohibits the
18 receiving covered entity from using the dis-
19 closed personal information for any purpose
20 other than provided in the contract; or

21 (2) the covered entity has—

22 (A) entered into an agreement with the re-
23 ceiving covered entity that—

24 (i) requires the receiving covered enti-
25 ty to comply with this division;

1 (ii) prohibits the receiving covered en-
2 tity from using the disclosed personal in-
3 formation for any purpose other than pro-
4 vided in the contract;

5 (iii) requires the receiving covered en-
6 tity to indemnify the covered entity against
7 violations of this division committed by the
8 receiving covered entity for any amount the
9 covered entity is unable to pay of a judg-
10 ment for such violation;

11 (iv) grants the covered entity the au-
12 thority to audit, including physical access
13 to electronic devices and data, the receiving
14 covered entity's compliance with this divi-
15 sion and the contract; and

16 (v) requires the receiving covered enti-
17 ty to assist the covered entity in respond-
18 ing to and complying with any court or-
19 ders, Agency orders, or the exercising of
20 an individual's rights under this division;

21 (B) actual knowledge that the receiving
22 covered entity is in compliance with this divi-
23 sion and not using personal information con-
24 trary to their agreement;

1 (C) actual knowledge that the receiving
2 covered entity is sufficiently solvent to com-
3 pensate victims or pay fines for violations of
4 this division;

5 (D) an auditing and compliance program
6 to ensure the receiving covered entity's contin-
7 ued compliance with this division and contract
8 terms;

9 (E) filed with the Agency the terms of said
10 contract, proof of its actual knowledge of the
11 receiving covered entity's compliance with this
12 division and contract terms, and documents de-
13 tailing its auditing and compliance program for
14 approval and publication by the Agency; and

15 (F) the covered entity has entered into an
16 agreement with the Agency where it agrees to
17 accept, respond to, or comply with a court
18 order, agency order, or request by an individual
19 regarding actions taken by the receiving covered
20 entity with respect to the data it has disclosed.

21 (d) For the purposes of subsection (c)(2), the covered
22 entity shall be jointly liable for a violation of this division
23 by the receiving covered entity regarding the data the cov-
24 ered entity disclosed, except where the covered entity was
25 the first to notify the Agency of the violation, in which

1 case, it shall be severally liable. Where the covered entity
2 should reasonably have known of a violation of this divi-
3 sion by the receiving covered entity and fails to disclose
4 the violation to the Agency, each day of continuance of
5 the failure to report such violation shall be treated as a
6 separate violation.

7 (e) AGENCY AGREEMENTS.—Upon the request of a
8 covered entity not subject to the jurisdiction of the United
9 States, the Agency shall enter into an agreement with the
10 covered entity that includes, but is not limited to, the fol-
11 lowing conditions:

12 (1) The principle place of business for the cov-
13 ered entity must be in a country that allows for the
14 domestication of a United States court decision for
15 civil fines payable to a government entity and in-
16 junctive relief. Where a foreign court refuses to en-
17 force a United States court decision under this divi-
18 sion, the agreement, and all other agreements with
19 covered entities with a principle place of business in
20 the same jurisdiction, shall be void.

21 (2) The covered entity agrees to comply with
22 this division.

23 (3) The covered entity agrees to be subject to
24 this division with choice of venue being a United
25 States court.

1 (4) The covered entity agrees to comply with
2 Agency investigative requests or orders, and United
3 States court orders or decisions under this division.

4 (5) The covered entity consents to United
5 States Federal court personal jurisdiction for the
6 sole purpose of enforcing this division.

7 (6) Where enforcement of the decision requires
8 the use of a foreign court, the covered entity agrees
9 to pay reasonable attorney fees necessary to enforce
10 the judgment.

11 (7) A default judgment, failure to comply with
12 Agency investigative requests or orders, or failure to
13 comply with United States court orders or decisions
14 shall result in the immediate termination of the
15 agreement.

16 (f) RULE OF CONSTRUCTION AGAINST DATA LOCAL-
17 IZATION.—Nothing in this section shall be construed to
18 require the localization of processing or maintaining per-
19 sonal information by a covered entity to within the United
20 State, or limit internal disclosure of personal information
21 within a covered entity or to subsidiary or corporate affil-
22 iate of such covered entity, regardless of the country in
23 which the covered entity will process, disclose, or maintain
24 that personal information.

1 **SEC. 206. PROHIBITION ON REIDENTIFICATION.**

2 (a) IN GENERAL.—Except as required under title I,
3 a covered entity shall not use personal information col-
4 lected from an individual, acquired from a third party, or
5 acquired from a publicly available information to reiden-
6 tify an individual from de-identified information.

7 (b) THIRD-PARTY PROHIBITION.—A covered entity
8 that discloses de-identified information to a third party
9 shall prohibit such third party from reidentifying an indi-
10 vidual using such de-identified information.

11 (c) EXCEPTION.—Subsection (a) shall not apply to
12 qualified research entities, as determined by the Director,
13 conducting research not for commercial purposes.

14 **SEC. 207. RESTRICTIONS ON COLLECTION, PROCESSING,**
15 **AND DISCLOSURE OF CONTENTS OF COMMU-**
16 **NICATIONS.**

17 (a) IN GENERAL.—A covered entity may not collect,
18 process, maintain, or disclose the contents of any commu-
19 nication, regardless of whether the sender or intended re-
20 cipient of the communication is an individual, other per-
21 son, or an electronic device, for any purpose other than—

22 (1) transmission or display of the communica-
23 tion to any intended recipient or the original sender,
24 or maintenance of such communications for such
25 purposes;

1 (2) detecting, responding to, or preventing secu-
2 rity incidents or threats;

3 (3) providing services to assist in the drafting
4 or creation of the content of a communication;

5 (4) processing expressly requested by the sender
6 or intended recipient, if the sender or intended re-
7 cipient can terminate such processing using a rea-
8 sonable mechanism;

9 (5) a disclosure otherwise required by law;

10 (6) the filtering of a communication where pri-
11 mary purpose of the communication is the commer-
12 cial advertisement or promotion of a commercial
13 product or service; or

14 (7) detecting or enforcing an abuse or violation
15 of the service's terms of service that would result in
16 either a temporary or permanent ban from using the
17 service.

18 (b) INTENDED RECIPIENT.—A covered entity is not
19 considered an intended recipient of a communication, or
20 any communication used in the creation of the content of
21 said communication, where—

22 (1) at least one intended recipient is a natural
23 person other than an employee or contractor of the
24 covered entity;

1 (2) at least one intended recipient is a person
2 other than the covered entity; or

3 (3) a purpose of the covered entity's service is
4 to maintain, at the direction of the sender, the con-
5 tent of said communication for more than a transi-
6 tory period.

7 (c) SENDER.—The sender of a communication is the
8 person for whom the communication, and its content, is
9 disclosed at the direction of and on behalf of.

10 (1) Where the sender is a natural person, they
11 shall be the sender of the entire content of the com-
12 munication, regardless of the original author of any
13 portion of the content.

14 (2) Otherwise, a sender shall be the sender of
15 only the content it was an original author of, or con-
16 tent it received as an intended recipient.

17 (d) EXCEPTION FOR PUBLICLY AVAILABLE COMMU-
18 NICATIONS.—Subsection (a) shall not apply where the con-
19 tents of communication that are made publicly accessible
20 by the sender without restrictions on accessibility other
21 than the general authorization to access the services used
22 to make the information accessible.

23 (e) ENCRYPTION PROTECTION.—A covered entity
24 shall not—

1 (1) prohibit or prevent a person from
2 encrypting or otherwise rendering unintelligible the
3 content of a communication using a means that pre-
4 vents the covered entity from being able to decrypt
5 or otherwise render intelligible said content; and

6 (2) require or cause a person to disclose or cir-
7 cumvent the means described in paragraph (1) to
8 the covered entity that would allow it to render the
9 content intelligible.

10 (f) **SERVICE PROVIDERS SAFE HARBOR.**—A service
11 provider shall not be held liable for a violation of this sec-
12 tion if such service provider is acting at the direction of
13 and on behalf of a covered entity and has a reasonable
14 belief that the covered entity’s directions are in compliance
15 with this section.

16 **SEC. 208. PROHIBITION ON DISCRIMINATORY PROCESSING.**

17 (a) **DISCRIMINATION IN ECONOMIC OPPORTUNI-**
18 **TIES.**—A covered entity shall not process personal infor-
19 mation or contents of communication for advertising, mar-
20 keting, soliciting, offering, selling, leasing, licensing, rent-
21 ing, or otherwise commercially contracting for employ-
22 ment, finance, healthcare, credit, insurance, housing, or
23 education opportunities in a manner that discriminates
24 against or otherwise makes opportunities unavailable on
25 the basis of an individual’s protected class status.

1 (b) PUBLIC ACCOMMODATIONS.—A covered entity
2 shall not process personal information in a manner that
3 segregates, discriminates in, or otherwise makes unavail-
4 able the goods, services, facilities, privileges, advantages,
5 or accommodations of any place of public accommodation
6 on the basis of a person’s or a group’s protected class sta-
7 tus.

8 (c) The Director shall promulgate regulations to im-
9 plement this section.

10 **SEC. 209. RESTRICTIONS ON GENETIC INFORMATION.**

11 (a) IN GENERAL.—A covered entity may not collect,
12 process, maintain, or disclose genetic information for any
13 purpose other than—

14 (1) providing medical treatment or testing to
15 the individual whose genetic information is being col-
16 lected, processed, maintained, or disclosed;

17 (2) research and services related to medical,
18 historical, or population uses of genetic information,
19 if, in the case of disclosure of genetic information—

20 (A) such genetic information is only dis-
21 closed to qualified research entities, as deter-
22 mined by the Director;

23 (B) additional personal information dis-
24 closed with such genetic information is limited

1 to the narrowest possible scope likely to yield
2 the intended benefit; and

3 (C) the covered entity limits, through con-
4 tractual obligations, additional types of personal
5 information that can be processed with the dis-
6 closed genetic information and personal infor-
7 mation.

8 (3) a purpose specified by the Director by regu-
9 lation, taking into account the potential privacy
10 harms and potential benefits of such collection, proc-
11 essing, maintenance, or disclosure; or

12 (4) to comply with a Federal criminal investiga-
13 tion request or order.

14 (b) GENETIC INFORMATION DEFINED.—In this sec-
15 tion, the term “genetic information” has the meaning
16 given such term in section 201 of the Genetic Information
17 Nondiscrimination Act of 2008 (42 U.S.C. 2000ff).

18 (c) SERVICE PROVIDERS SAFE HARBOR.—A service
19 provider shall not be held liable for a violation of this sec-
20 tion if such service provider is acting at the direction of
21 and on behalf of a covered entity and has a reasonable
22 belief that is the covered entity’s directions are in compli-
23 ance with this section.

1 **SEC. 210. REQUIREMENTS FOR NOTICE AND CONSENT**
2 **PROCESSES AND PRIVACY POLICIES.**

3 (a) **MINIMUM THRESHOLD.**—The Director shall es-
4 tablish a minimum threshold that a covered entity must
5 meet for the percentage of individuals who read and un-
6 derstand a notice or consent process or privacy policy re-
7 quired by this division. In establishing such minimum
8 thresholds, the Director shall take into account expecta-
9 tions of individuals, potential privacy harms, and individ-
10 uals' awareness of privacy harms.

11 (b) **CONSENT REVOCATION.**—A covered entity shall
12 make available a reasonable mechanism by which an indi-
13 vidual may revoke consent for any consent given under
14 this division.

15 (c) **SAFE HARBOR.**—

16 (1) **APPROVAL PROCEDURES.**—The Director
17 shall develop procedures for analyzing and approving
18 data submitted by a covered entity to establish that
19 a notice and consent process or privacy policy of
20 such covered entity meets the threshold established
21 under subsection (a).

22 (2) **PRESUMPTION.**—If a covered entity submits
23 testing data to and receives an approval from the
24 Director under paragraph (1) establishing that a no-
25 tice or consent process or privacy policy of such cov-
26 ered entity meets the threshold established under

1 subsection (a), such notice or consent process or pri-
2 vacy policy shall be presumed to have met such
3 threshold. Such presumption may be rebutted by
4 clear and convincing evidence.

5 (3) PUBLIC AVAILABILITY OF APPROVED PROC-
6 ESSES AND POLICIES AND ASSOCIATED TESTING
7 DATA.—The Director shall make publicly available
8 online the notice and consent processes and privacy
9 policies and associated testing data that the Director
10 approves under paragraph (1).

11 (4) SMALL BUSINESS ADOPTION OF NOTICE OR
12 CONSENT PROCESS OF ANOTHER COVERED ENTI-
13 TY.—

14 (A) IN GENERAL.—If a small business
15 adopts a notice or consent process of another
16 covered entity that collects, processes, main-
17 tains, or discloses personal information in sub-
18 stantially the same way as such small business,
19 if the process of such other covered entity has
20 been approved under paragraph (1), the process
21 of such small business shall receive the pre-
22 sumption under paragraph (2).

23 (B) ABILITY TO FREELY USE APPROVED
24 PROCESS.—A covered entity whose notice or
25 consent process is approved under paragraph

1 (1) shall permit a small business to freely use
2 such process, or a derivative thereof, as de-
3 scribed in subparagraph (A).

4 (C) NO PUBLISHED PROCESS.—In the case
5 of a small business for which there is no ap-
6 proved notice or consent process published
7 under paragraph (3) of a covered entity that
8 collects, processes, maintains, or discloses per-
9 sonal information in substantially the same way
10 as such small business, any requirement under
11 this title for a notice or consent process to be
12 objectively shown to meet the threshold estab-
13 lished by the Director under subsection (a)
14 shall not apply to such small business. Nothing
15 in the preceding sentence exempts a small busi-
16 ness from the requirement to use such notice or
17 consent process or that such process be concise
18 and clear.

19 (D) INAPPLICABILITY TO PRIVACY POL-
20 ICY.—Paragraph (4) does not apply with re-
21 spect to a privacy policy.

22 (5) MINOR CHANGES.—A covered entity may
23 make minor changes in a notice or consent process
24 or privacy policy approved under paragraph (1) and
25 retain the presumption under paragraph (2) for such

1 process or policy without retesting or resubmission
2 of testing data to the Director.

3 **SEC. 211. PROHIBITION ON DECEPTIVE NOTICE AND CON-**
4 **SENT PROCESSES AND PRIVACY POLICIES.**

5 In providing notice, obtaining consent, or maintaining
6 a privacy policy as required by this title, a covered entity
7 may not intentionally take any action that substantially
8 impairs, obscures, or subverts the ability of an individual
9 to—

10 (1) understand the contents of such notice or
11 such privacy policy;

12 (2) understand the process for granting such
13 consent;

14 (3) make a decision regarding whether to grant
15 or withdraw such consent; or

16 (4) act on any such decision.

17 **SEC. 212. NOTICE AND CONSENT REQUIRED.**

18 (a) NOTICE.—A covered entity shall provide an indi-
19 vidual with notice of the personal information such covered
20 entity collects, processes, maintains, and discloses through
21 a process that is concise and clear and can be objectively
22 shown to meet the threshold established by the Director
23 under section 210(a).

24 (b) CONSENT.—

1 (1) EXPRESS CONSENT REQUIRED.—Except as
2 provided in paragraphs (2) and (3), a covered entity
3 may not collect from an individual personal informa-
4 tion that creates or increases the risk of foreseeable
5 privacy harms, or process or maintain any such per-
6 sonal information collected from an individual, un-
7 less such entity obtains the express consent of such
8 individual to the collection, processing, or mainte-
9 nance (or any combination thereof) of such informa-
10 tion through a process that is concise and clear and
11 can be objectively shown to meet the threshold es-
12 tablished by the Director under section 210(a).

13 (2) EXCEPTION FOR IMPLIED CONSENT.—Not-
14 withstanding paragraph (1), express consent is not
15 required for collection, processing, or maintenance of
16 personal information if the collection, processing, or
17 maintenance is, on its face, obvious and necessary to
18 provide a service at the request of the individual and
19 the personal information is collected, processed, or
20 maintained only for such request. Nothing in this
21 paragraph shall be construed to exempt the covered
22 entity from the requirement of subsection (a) to pro-
23 vide notice to such individual with respect to such
24 collection, processing, or maintenance.

1 (3) EXEMPTION FOR PRIVACY PRESERVING
2 COMPUTING.—Notwithstanding paragraph (1), ex-
3 cept with regard to consent for purposes of section
4 106, express consent is not required for collection,
5 processing, or maintenance of personal information
6 secured using privacy preserving computing. Nothing
7 in this paragraph shall be construed to exempt the
8 covered entity from the requirement of subsection
9 (a) to provide notice to such individual with respect
10 to such collection, processing, or maintenance.

11 (c) SERVICE PROVIDERS EXCLUDED.—This section
12 does not apply to a service provider if such service provider
13 has a reasonable belief that a covered entity for which it
14 processes, maintains, or discloses personal information is
15 in compliance with this section.

16 **SEC. 213. PRIVACY POLICY.**

17 (a) POLICY REQUIRED.—A covered entity shall main-
18 tain a privacy policy relating to the practices of such entity
19 regarding the collection, processing, maintenance, and dis-
20 closure of personal information.

21 (b) CONTENTS.—The privacy policy required by sub-
22 section (a) shall contain the following:

23 (1) A general description of the practices of the
24 covered entity regarding the collection, processing,
25 maintenance, and disclosure of personal information.

1 (2) A description of how individuals may exer-
2 cise the rights provided by title I.

3 (3) A clear and concise summary of the fol-
4 lowing:

5 (A) The categories of personal information
6 collected or otherwise obtained by the covered
7 entity.

8 (B) The business or commercial purposes
9 of the covered entity for collecting, processing,
10 maintaining, or disclosing personal information.

11 (C) The categories and a list of third par-
12 ties to which the covered entity discloses per-
13 sonal information.

14 (4) A description of the personal information
15 that the covered entity maintains that the covered
16 entity does not collect from individuals and how the
17 covered entity obtains such personal information.

18 (5) A list of the third parties to which the cov-
19 ered entity has disclosed personal information.

20 (6) A list of the third parties from which the
21 covered entity has obtained personal information at
22 any time on or after the effective date specified in
23 section 4(a).

1 (7) The articulated basis for the collection,
2 processing, disclosure and maintenance of personal
3 information, as required under section 201(a).

4 (c) EXEMPTION FOR PERSONAL INFORMATION FOR
5 PARTICULAR PURPOSES.—The privacy policy required by
6 subsection (a) is not required to contain information relat-
7 ing to personal information that is collected, processed,
8 maintained, or disclosed exclusively for any of the pur-
9 poses described in paragraph (1) of section 109(a) (or a
10 combination of such purposes), except as provided in para-
11 graph (2) of such section.

12 (d) AVAILABILITY OF PRIVACY POLICY.—

13 (1) FORM AND MANNER.—The privacy policy
14 required by subsection (a) shall be—

15 (A) clear and in plain language; and

16 (B) made publicly available in a prominent
17 location on an ongoing basis.

18 (2) TIMING.—The privacy policy required by
19 subsection (a) shall be made available as required by
20 paragraph (1) before any collection of personal in-
21 formation by the covered entity that occurs after the
22 effective date specified in section 4(a).

23 (e) SMALL BUSINESSES EXCLUDED.—Subsections
24 (b)(7) and (d) do not apply to a small business.

1 (f) SERVICE PROVIDERS EXCLUDED.—This section
2 does not apply to a service provider if such service provider
3 has a reasonable belief that a covered entity for which it
4 processes, maintains, or discloses personal information is
5 in compliance with this section.

6 **SEC. 214. INFORMATION SECURITY REQUIREMENTS.**

7 (a) IN GENERAL.—A covered entity shall establish
8 and implement reasonable information security policies,
9 practices, and procedures for the protection of personal
10 information collected, processed, maintained, or disclosed
11 by such covered entity, taking into consideration—

12 (1) the nature, scope, and complexity of the ac-
13 tivities engaged in by such covered entity;

14 (2) the sensitivity of any personal information
15 at issue;

16 (3) the current state of the art in administra-
17 tive, technical, and physical safeguards for pro-
18 tecting such information; and

19 (4) the cost of implementing such administra-
20 tive, technical, and physical safeguards.

21 (b) POINT OF CONTACT.—A covered entity shall iden-
22 tify an officer or other individual as the point of contact
23 with responsibility for the management of information se-
24 curity.

1 (c) SPECIFIC POLICIES, PRACTICES, AND PROCE-
2 DURES.—The policies, practices, and procedures required
3 by subsection (a) shall include the following:

4 (1) A written security policy with respect to the
5 collection, processing, maintenance, and disclosure of
6 personal information. Such policy shall be made pub-
7 licly available in a prominent location on an ongoing
8 basis, except that the publicly available version is
9 not required to contain information that would com-
10 promise a purpose described in paragraph (1) of sec-
11 tion 109(a).

12 (2) A process for identifying and assessing rea-
13 sonably foreseeable security vulnerabilities in the
14 system or systems used by such covered entity that
15 contain personal information, which shall include
16 regular monitoring for vulnerabilities or data
17 breaches involving such system or systems.

18 (3) A process for taking action designed to
19 mitigate against vulnerabilities identified in the
20 process required by paragraph (2), which may in-
21 clude implementing any changes to security practices
22 and the architecture, installation, or implementation
23 of network or operating software, or for regularly
24 testing or otherwise monitoring the effectiveness of
25 the existing safeguards.

1 (4) A process for determining if personal infor-
2 mation is no longer needed and disposing of personal
3 information by shredding, permanently erasing, or
4 otherwise modifying the medium on which such per-
5 sonal information is maintained to make such per-
6 sonal information permanently unreadable or indeci-
7 pherable.

8 (5) A process for overseeing persons who have
9 access to personal information, including through
10 network-connected devices.

11 (6) A process for employee training and super-
12 vision for implementation of the policies, practices,
13 and procedures required by this section.

14 (7) A written plan or protocol for internal and
15 public response in the event of a data breach or data
16 sharing abuse.

17 (d) REGULATIONS.—The Director, in consultation
18 with the National Institute of Standards and Technology,
19 shall promulgate regulations to implement this section.

20 (e) SMALL BUSINESSES ASSISTANCE.—The Director,
21 in consultation with the National Institute of Standards
22 and Technology, the Small Business Association, and
23 small businesses, shall develop policy templates, toolkits,
24 tip sheets, configuration guidelines for commonly used
25 hardware and software, interactive tools, and other mate-

1 rials to assist small businesses with complying with this
2 section.

3 **SEC. 215. NOTIFICATION OF DATA BREACH OR DATA SHAR-**
4 **ING ABUSE.**

5 (a) NOTIFICATION OF AGENCY.—

6 (1) IN GENERAL.—In the case of a data breach
7 or data sharing abuse with respect to personal infor-
8 mation maintained by a covered entity, such covered
9 entity shall, without undue delay and, if feasible, not
10 later than 72 hours after becoming aware of such
11 data breach or data sharing abuse, notify the Direc-
12 tor of such data breach or data sharing abuse, un-
13 less such data breach or data sharing abuse is un-
14 likely to create or increase foreseeable privacy
15 harms.

16 (2) REASONS FOR DELAY.—If the notification
17 required by paragraph (1) is made more than 72
18 hours after the covered entity becomes aware of the
19 data breach or data sharing abuse, such notification
20 shall be accompanied by a statement of the reasons
21 for the delay.

22 (b) NOTIFICATION OF OTHER COVERED ENTITY.—
23 In the case of a data breach or data sharing abuse with
24 respect to personal information maintained by a covered
25 entity that such covered entity obtained from another cov-

1 ered entity, the covered entity experiencing such data
2 breach or data sharing abuse shall, without undue delay
3 and, if feasible, not later than 72 hours after becoming
4 aware of such data breach or data sharing abuse, notify
5 such other covered entity of such data breach or data
6 sharing abuse, unless such data breach or data sharing
7 abuse is unlikely to create or increase foreseeable privacy
8 harms. A covered entity receiving notice under this sub-
9 section of a data breach or data sharing abuse shall notify
10 any other covered entity from which the covered entity re-
11 ceiving notice obtained personal information involved in
12 such data breach or data sharing abuse, in the same man-
13 ner as required under the preceding sentence for the cov-
14 ered entity experiencing such data breach or data sharing
15 abuse.

16 (c) NOTIFICATION OF INDIVIDUALS.—

17 (1) IN GENERAL.—In the case of a data breach
18 or data sharing abuse with respect to personal infor-
19 mation maintained by a covered entity (or a data
20 breach or data sharing abuse about which a covered
21 entity is notified under subsection (b)), if such cov-
22 ered entity has a relationship with an individual
23 whose personal information was involved or poten-
24 tially involved in such data breach or data sharing
25 abuse, such covered entity shall notify such indi-

1 vidual of such data breach or data sharing abuse not
2 later than 14 days after becoming aware of such
3 data breach or data sharing abuse (or, in the case
4 of a data breach or data sharing abuse about which
5 a covered entity is notified under subsection (b), not
6 later than 14 days after being so notified), if such
7 data breach or data sharing abuse creates or in-
8 creases foreseeable privacy harms.

9 (2) MEDIUM OF NOTIFICATION.—A covered en-
10 tity shall notify an individual as required by para-
11 graph (1) through—

12 (A) the same medium through which such
13 individual routinely interacts with such covered
14 entity; and

15 (B) one additional medium of notification,
16 if such covered entity has the personal informa-
17 tion necessary to make a notification through
18 such an additional medium without causing ex-
19 cessive financial burden for such covered entity.

20 (d) RULE OF CONSTRUCTION.—This section shall not
21 apply to a covered entity if a person uses personal infor-
22 mation obtained from a data breach or data sharing abuse
23 not involving such covered entity.

1 **TITLE III—UNITED STATES**
2 **DIGITAL PRIVACY AGENCY**

3 **SEC. 301. ESTABLISHMENT.**

4 (a) **AGENCY ESTABLISHED.**—There is established an
5 independent agency in the executive branch to be known
6 as the “United States Digital Privacy Agency”, which
7 shall implement and enforce this division.

8 (b) **DIRECTOR AND DEPUTY DIRECTOR.**—

9 (1) **IN GENERAL.**—There is established the po-
10 sition of the Director, who shall serve as the head
11 of the Agency.

12 (2) **APPOINTMENT.**—Subject to paragraph (3),
13 the Director shall be appointed by the President, by
14 and with the advice and consent of the Senate.

15 (3) **QUALIFICATION.**—The President shall
16 nominate the Director from among individuals who
17 are citizens of the United States.

18 (4) **DEPUTY DIRECTOR.**—There is established
19 the position of Deputy Director, who shall—

20 (A) be appointed by the Director; and

21 (B) serve as acting Director in the absence
22 or unavailability of the Director.

23 (c) **TERM.**—

24 (1) **IN GENERAL.**—The Director shall serve for
25 a term of 5 years.

1 (2) EXPIRATION OF TERM.—An individual may
2 serve as Director after the expiration of the term for
3 which appointed, until a successor has been ap-
4 pointed and qualified.

5 (3) REMOVAL FOR CAUSE.—The President may
6 remove the Director for inefficiency, neglect of duty,
7 or malfeasance in office.

8 (d) SERVICE RESTRICTION.—No Director or Deputy
9 Director may hold any office, position, or employment in
10 any covered entity during the period of service of such per-
11 son as Director or Deputy Director.

12 (e) OFFICES.—The Director shall establish a prin-
13 cipal office and field offices of the Agency in locations that
14 have high levels of activity by covered entities, as deter-
15 mined by the Director.

16 (f) COMPENSATION.—

17 (1) IN GENERAL.—The Director shall be com-
18 pensated at the rate prescribed for level II of the
19 Executive Schedule under section 5313 of title 5,
20 United States Code.

21 (2) CONFORMING AMENDMENT.—Section 5313
22 of title 5, United States Code, is amended by insert-
23 ing after the item relating to “Federal Transit Ad-
24 ministrator.” the following new item: “Director of
25 the United States Digital Privacy Agency.”.

1 **SEC. 302. EXECUTIVE AND ADMINISTRATIVE POWERS.**

2 (a) POWERS OF THE AGENCY.—The Director is au-
3 thorized to establish the general policies of the Agency
4 with respect to all executive and administrative functions,
5 including—

6 (1) the establishment of rules for conducting
7 the general business of the Agency, in a manner not
8 inconsistent with this division;

9 (2) to bind the Agency and enter into contracts;

10 (3) directing the establishment and mainte-
11 nance of divisions or other offices within the Agency,
12 in order to carry out the responsibilities of the Agen-
13 cy under this division, and to satisfy the require-
14 ments of other applicable law;

15 (4) to coordinate and oversee the operation of
16 all administrative, enforcement, and research activi-
17 ties of the Agency;

18 (5) to adopt and use a seal;

19 (6) to determine the character of and the neces-
20 sity for the obligations and expenditures of the
21 Agency;

22 (7) the appointment and supervision of per-
23 sonnel employed by the Agency;

24 (8) the distribution of business among per-
25 sonnel appointed and supervised by the Director and
26 among administrative units of the Agency;

1 (9) the use and expenditure of funds;

2 (10) implementing this division through rules,
3 orders, guidance, interpretations, statements of pol-
4 icy, investigations, and enforcement actions; and

5 (11) performing such other functions as may be
6 authorized or required by law.

7 (b) DELEGATION OF AUTHORITY.—The Director
8 may delegate to any duly authorized employee, representa-
9 tive, or agent any power vested in the Director or the
10 Agency by law, except that the Director may not delegate
11 the power to appoint the Deputy Director under section
12 301(b)(4)(A).

13 (c) AUTONOMY OF AGENCY REGARDING REC-
14 OMMENDATIONS AND TESTIMONY.—No officer or agency
15 of the United States shall have any authority to require
16 the Director or any other officer of the Agency to submit
17 legislative recommendations, or testimony or comments on
18 legislation, to any officer or agency of the United States
19 for approval, comments, or review prior to the submission
20 of such recommendations, testimony, or comments to the
21 Congress, if such recommendations, testimony, or com-
22 ments to the Congress include a statement indicating that
23 the views expressed therein are those of the Director or
24 such officer, and do not necessarily reflect the views of
25 the President.

1 **SEC. 303. RULEMAKING AUTHORITY.**

2 The Director may prescribe rules and issue orders
3 and guidance, as may be necessary or appropriate to en-
4 able the Agency to administer and carry out the purposes
5 and objectives of this division, and to prevent evasions
6 thereof.

7 **SEC. 304. PERSONNEL.**

8 (a) APPOINTMENT.—

9 (1) IN GENERAL.—The Director may fix the
10 number of, and appoint and direct, all employees of
11 the Agency, in accordance with the applicable provi-
12 sions of title 5, United States Code.

13 (2) EMPLOYEES OF THE AGENCY.—The Direc-
14 tor is authorized to employ technologists, designers,
15 attorneys, investigators, economists, and other em-
16 ployees as the Director considers necessary to con-
17 duct the business of the Agency.

18 (b) AGENCY OMBUDSMAN.—

19 (1) ESTABLISHMENT REQUIRED.—The Director
20 shall appoint an ombudsman.

21 (2) DUTIES OF OMBUDSMAN.—The ombudsman
22 appointed in accordance with paragraph (1) shall—

23 (A) act as a liaison between the Agency
24 and any affected person with respect to any
25 problem that such person may have in dealing

1 with the Agency, resulting from the regulatory
2 activities of the Agency; and

3 (B) assure that safeguards exist to encour-
4 age complainants to come forward and preserve
5 confidentiality.

6 **SEC. 305. COMPLAINTS OF INDIVIDUALS.**

7 (a) IN GENERAL.—The Director shall establish a unit
8 within the Agency the functions of which shall include es-
9 tablishing a single, toll-free telephone number, a website,
10 and a database or utilizing an existing database to facili-
11 tate the centralized collection of, monitoring of, and re-
12 sponse to complaints of individuals regarding the privacy
13 or security of personal information. The Director shall co-
14 ordinate with other Federal agencies with jurisdiction over
15 the privacy or security of personal information to route
16 complaints to such agencies, where appropriate.

17 (b) ROUTING COMPLAINTS TO STATES.—To the ex-
18 tent practicable, State agencies may receive appropriate
19 complaints from the systems established under subsection
20 (a), if—

21 (1) the State agency system has the functional
22 capacity to receive calls or electronic reports routed
23 by the Agency systems;

24 (2) the State agency has satisfied any condi-
25 tions of participation in the system that the Agency

1 may establish, including treatment of personal infor-
2 mation and sharing of information on complaint res-
3 olution or related compliance procedures and re-
4 sources; and

5 (3) participation by the State agency includes
6 measures necessary to provide for protection of per-
7 sonal information that conform to the standards for
8 protection of the confidentiality of personal informa-
9 tion and for data integrity and security that apply
10 to Federal agencies.

11 (c) DATA SHARING REQUIRED.—To facilitate inclu-
12 sion in the reports required by section 310 of the matters
13 regarding complaints of individuals required by subsection
14 (b)(4) of such section to be included in such reports, inves-
15 tigation and enforcement activities, and monitoring of the
16 privacy and security of personal information, the Agency
17 shall share information about complaints of individuals
18 with Federal and State agencies that have jurisdiction
19 over the privacy or security of personal information and
20 State attorneys general, subject to the standards applica-
21 ble to Federal agencies for protection of the confidentiality
22 of personal information and for data security and integ-
23 rity. Other Federal agencies that have jurisdiction over the
24 privacy or security of personal information shall share
25 data relating to complaints of individuals regarding the

1 privacy or security of personal information with the Agen-
2 cy, subject to the standards applicable to Federal agencies
3 for protection of confidentiality of personal information
4 and for data security and integrity.

5 **SEC. 306. USER ADVISORY BOARD.**

6 (a) ESTABLISHMENT REQUIRED.—The Director shall
7 establish a User Advisory Board to advise and consult
8 with the Agency in the exercise of its functions under this
9 division, and to provide information on emerging practices
10 relating to the treatment of personal information by cov-
11 ered entities, including regional trends, concerns, and
12 other relevant information.

13 (b) MEMBERSHIP.—In appointing the members of
14 the User Advisory Board, the Director shall seek to assem-
15 ble experts in consumer protection, privacy, civil rights,
16 and ethics, and seek representation of the interests of indi-
17 viduals who use products or services provided by covered
18 entities, without regard to party affiliation.

19 (c) MEETINGS.—The User Advisory Board shall meet
20 from time to time at the call of the Director, but, at a
21 minimum, shall meet at least twice in each year.

22 (d) COMPENSATION AND TRAVEL EXPENSES.—Mem-
23 bers of the User Advisory Board who are not full-time em-
24 ployees of the United States shall—

1 (1) be entitled to receive compensation at a rate
2 fixed by the Director while attending meetings of the
3 User Advisory Board, including travel time; and

4 (2) receive travel expenses, including per diem
5 in lieu of subsistence, in accordance with applicable
6 provisions under subchapter I of chapter 57 of title
7 5, United States Code.

8 **SEC. 307. ACADEMIC AND RESEARCH ADVISORY BOARD.**

9 (a) ESTABLISHMENT REQUIRED.—The Director shall
10 establish an Academic and Research Advisory Board to
11 advise and consult with the Agency in the exercise of its
12 functions under this division, and to provide information
13 on emerging practices relating to the treatment of per-
14 sonal information by covered entities, including regional
15 trends, concerns, and other relevant information.

16 (b) MEMBERSHIP.—In appointing the members of
17 the Academic and Research Advisory Board, the Director
18 shall seek to assemble individuals with academic and re-
19 search expertise in privacy, cybersecurity, computer
20 science, innovation, economics, law, and public policy,
21 without regard to party affiliation.

22 (c) MEETINGS.—The Academic and Research Advi-
23 sory Board shall meet from time to time at the call of
24 the Director, but, at a minimum, shall meet at least twice
25 in each year.

1 (d) COMPENSATION AND TRAVEL EXPENSES.—Mem-
2 bers of the Academic and Research Advisory Board who
3 are not full-time employees of the United States shall—

4 (1) be entitled to receive compensation at a rate
5 fixed by the Director while attending meetings of the
6 Academic and Research Advisory Board, including
7 travel time; and

8 (2) receive travel expenses, including per diem
9 in lieu of subsistence, in accordance with applicable
10 provisions under subchapter I of chapter 57 of title
11 5, United States Code.

12 **SEC. 308. SMALL BUSINESS AND INVESTOR ADVISORY**
13 **BOARD.**

14 (a) ESTABLISHMENT REQUIRED.—The Director shall
15 establish a Small Business and Investor Advisory Board
16 to advise and consult with the Agency in the exercise of
17 its functions under this division, and to provide informa-
18 tion on emerging practices relating to the treatment of
19 personal information by covered entities, including re-
20 gional trends, concerns, and other relevant information.

21 (b) MEMBERSHIP.—In appointing the members of
22 the Small Business and Investor Advisory Board, the Di-
23 rector shall seek to assemble representatives of small busi-
24 nesses and investors in small businesses, without regard
25 to party affiliation.

1 (c) MEETINGS.—The Small Business and Investor
2 Advisory Board shall meet from time to time at the call
3 of the Director, but, at a minimum, shall meet at least
4 twice in each year.

5 (d) COMPENSATION AND TRAVEL EXPENSES.—Mem-
6 bers of the Small Business and Investor Advisory Board
7 who are not full-time employees of the United States
8 shall—

9 (1) be entitled to receive compensation at a rate
10 fixed by the Director while attending meetings of the
11 Small Business and Investor Advisory Board, includ-
12 ing travel time; and

13 (2) receive travel expenses, including per diem
14 in lieu of subsistence, in accordance with applicable
15 provisions under subchapter I of chapter 57 of title
16 5, United States Code.

17 **SEC. 309. CONSULTATION.**

18 The Director shall consult with Federal and State
19 agencies that have jurisdiction over the privacy or security
20 of personal information, State attorneys general, inter-
21 national and intergovernmental bodies that conduct activi-
22 ties relating to the privacy or security of personal informa-
23 tion, and agencies of other countries that are similar to
24 the Agency, as appropriate, to promote consistent regu-

1 latory treatment of the activities of covered entities relat-
2 ing to the privacy or security of personal information.

3 **SEC. 310. REPORTS.**

4 (a) **REPORTS REQUIRED.**—Not later than 6 months
5 after the date of the enactment of this Act, and every 6
6 months thereafter, the Director shall submit a report to
7 the President and to the Committee on Energy and Com-
8 merce, the Committee on the Judiciary, and the Com-
9 mittee on Appropriations of the House of Representatives
10 and the Committee on Commerce, Science, and Transpor-
11 tation, the Committee on the Judiciary, and the Com-
12 mittee on Appropriations of the Senate, and shall publish
13 such report on the website of the Agency.

14 (b) **CONTENTS.**—Each report required by subsection
15 (a) shall include—

16 (1) a discussion of the significant problems
17 faced by individuals with respect to the privacy or
18 security of personal information;

19 (2) a justification of the budget request of the
20 Agency for the preceding year, unless a justification
21 for such year was included in the preceding report
22 submitted under such subsection;

23 (3) a list of the significant rules and orders
24 adopted by the Agency, as well as other significant
25 initiatives conducted by the Agency, during the pre-

1 ceding 6-month period and the plan of the Agency
2 for rules, orders, or other initiatives to be under-
3 taken during the upcoming 6-month period;

4 (4) an analysis of complaints about the privacy
5 or security of personal information that the Agency
6 has received and collected in the database described
7 in section 305(a) during the preceding 6-month pe-
8 riod;

9 (5) a list, with a brief statement of the issues,
10 of the public enforcement actions to which the Agen-
11 cy was a party during the preceding 6-month period;
12 and

13 (6) an assessment of significant actions by
14 State attorneys general or State agencies relating to
15 this division or the rules prescribed under this divi-
16 sion during the preceding 6-month period.

17 **SEC. 311. GRANTS FOR DEVELOPING OPEN-SOURCE MA-**
18 **CHINE LEARNING TRAINING DATA.**

19 The Director shall establish an Open-Source Machine
20 Learning Training Data Program and make grants
21 through the program to support the development of open-
22 source, voluntarily disclosed, personal information data
23 sets to be used for the training or development of machine
24 learning and artificial intelligence algorithms. The Direc-
25 tor shall promulgate regulations to implement the Pro-

1 gram and to consider any such data sets are in compliance
2 with this division balancing any intrusion on the privacy
3 of, potential privacy harms to, and reasonable expectations
4 of individuals to whom the personal information relates.

5 **SEC. 312. ANNUAL AUDITS.**

6 The Director shall order an annual independent audit
7 of the operations and budget of the Agency.

8 **SEC. 313. INSPECTOR GENERAL.**

9 Section 12 of the Inspector General Act of 1978 (5
10 U.S.C. App.) is amended—

11 (1) in paragraph (1), by inserting the “Director
12 of the Digital Privacy Agency;” after “the President
13 of the Export-Import Bank;”; and

14 (2) in paragraph (2), by inserting “the Digital
15 Privacy Agency,” after “the Export-Import Bank,”.

16 **SEC. 314. AUTHORIZATION OF APPROPRIATIONS.**

17 There are authorized to be appropriated to the Direc-
18 tor to carry out this division \$550,000,000 for each of
19 the fiscal years 2022, 2023, 2024, 2025, and 2026.

20 **TITLE IV—ENFORCEMENT**

21 **SEC. 401. DEFINITIONS.**

22 In this title:

23 (1) AGENCY INVESTIGATOR.—The term “Agen-
24 cy investigator” means any attorney or investigator
25 employed by the Agency who is charged with the

1 duty of enforcing or carrying into effect any provi-
2 sion of this division or a rule or order prescribed
3 under this division.

4 (2) ATTORNEY GENERAL.—The term “attorney
5 general” means, with respect to a State, the attor-
6 ney general or chief law enforcement officer of the
7 State, or another official or agency designated by
8 the State to bring civil actions on behalf of the State
9 or the residents of the State.

10 (3) CUSTODIAN.—The term “custodian” means
11 the custodian or any deputy custodian designated by
12 the Agency.

13 (4) DOCUMENTARY MATERIAL.—The term
14 “documentary material” includes the original or any
15 copy of any book, document, record, report, memo-
16 randum, paper, communication, tabulation, chart,
17 logs, electronic files, or other data or data compila-
18 tions stored in any medium.

19 (5) VIOLATION.—The term “violation” means
20 any act or omission that, if proved, would constitute
21 a violation of any provision of this division or a rule
22 or order prescribed under this division.

23 (6) NON-PUBLIC INFORMATION.—The term
24 “non-public information” means information that
25 has not been disclosed in a criminal, civil, or admin-

1 and give testimony or to appear and produce docu-
2 ments or other material.

3 (3) CONTEMPT.—Any failure to obey an order
4 of the court under paragraph (2) may be punished
5 by the court as a contempt thereof.

6 (c) DEMANDS.—

7 (1) IN GENERAL.—Whenever the Agency has
8 reason to believe that any person may be in posses-
9 sion, custody, or control of any documentary mate-
10 rial or tangible things, or may have any information,
11 relevant to a violation, the Agency may, before the
12 institution of any proceedings under this division,
13 issue in writing, and cause to be served upon such
14 person, a civil investigative demand requiring such
15 person to—

16 (A) produce such documentary material for
17 inspection and copying or reproduction in the
18 form or medium requested by the Agency;

19 (B) submit such tangible things;

20 (C) file written reports or answers to ques-
21 tions;

22 (D) give oral testimony concerning docu-
23 mentary material, tangible things, or other in-
24 formation; or

1 (E) furnish any combination of such mate-
2 rial, answers, or testimony.

3 (2) REQUIREMENTS.—Each civil investigative
4 demand shall state the nature of the conduct consti-
5 tuting the alleged violation which is under investiga-
6 tion and the provision of law applicable to such vio-
7 lation.

8 (3) PRODUCTION OF DOCUMENTS.—Each civil
9 investigative demand for the production of documen-
10 tary material shall—

11 (A) describe each class of documentary
12 material to be produced under the demand with
13 such definiteness and certainty as to permit
14 such material to be fairly identified;

15 (B) prescribe a return date or dates which
16 will provide a reasonable period of time within
17 which the material so demanded may be assem-
18 bled and made available for inspection and
19 copying or reproduction; and

20 (C) identify the custodian to whom such
21 material shall be made available.

22 (4) PRODUCTION OF THINGS.—Each civil inves-
23 tigative demand for the submission of tangible
24 things shall—

1 (A) describe each class of tangible things
2 to be submitted under the demand with such
3 definiteness and certainty as to permit such
4 things to be fairly identified;

5 (B) prescribe a return date or dates which
6 will provide a reasonable period of time within
7 which the things so demanded may be assem-
8 bled and submitted; and

9 (C) identify the custodian to whom such
10 things shall be submitted.

11 (5) DEMAND FOR WRITTEN REPORTS OR AN-
12 SWERS.—Each civil investigative demand for written
13 reports or answers to questions shall—

14 (A) propound with definiteness and cer-
15 tainty the reports to be produced or the ques-
16 tions to be answered;

17 (B) prescribe a date or dates at which time
18 written reports or answers to questions shall be
19 submitted; and

20 (C) identify the custodian to whom such
21 reports or answers shall be submitted.

22 (6) ORAL TESTIMONY.—Each civil investigative
23 demand for the giving of oral testimony shall—

24 (A) prescribe a date, time, and place at
25 which oral testimony shall be commenced; and

1 (B) identify an Agency investigator who
2 shall conduct the investigation and the custo-
3 dian to whom the transcript of such investiga-
4 tion shall be submitted.

5 (7) SERVICE.—Any civil investigative demand
6 issued, and any enforcement petition filed, under
7 this section may be served—

8 (A) by any Agency investigator at any
9 place within the territorial jurisdiction of any
10 court of the United States; and

11 (B) upon any person who is not found
12 within the territorial jurisdiction of any court of
13 the United States—

14 (i) in such manner as the Federal
15 Rules of Civil Procedure prescribe for serv-
16 ice in a foreign nation; and

17 (ii) to the extent that the courts of
18 the United States have authority to assert
19 jurisdiction over such person, consistent
20 with due process, the United States Dis-
21 trict Court for the District of Columbia
22 shall have the same jurisdiction to take
23 any action respecting compliance with this
24 section by such person that such district
25 court would have if such person were per-

1 sonally within the jurisdiction of such dis-
2 trict court.

3 (8) METHOD OF SERVICE.—Service of any civil
4 investigative demand or any enforcement petition
5 filed under this section may be made upon a person
6 by—

7 (A) delivering a duly executed copy of such
8 demand or petition to the individual or to any
9 partner, executive officer, managing agent, or
10 general agent of such person, or to any agent
11 of such person authorized by appointment or by
12 law to receive service of process on behalf of
13 such person;

14 (B) delivering a duly executed copy of such
15 demand or petition to the principal office or
16 place of business of the person to be served; or

17 (C) depositing a duly executed copy in the
18 United States mails, by registered or certified
19 mail, return receipt requested, duly addressed
20 to such person at the principal office or place
21 of business of such person.

22 (9) PROOF OF SERVICE.—

23 (A) IN GENERAL.—A verified return by the
24 individual serving any civil investigative demand
25 or any enforcement petition filed under this sec-

1 tion setting forth the manner of such service
2 shall be proof of such service.

3 (B) RETURN RECEIPTS.—In the case of
4 service by registered or certified mail, such re-
5 turn shall be accompanied by the return post
6 office receipt of delivery of such demand or en-
7 forcement petition.

8 (10) PRODUCTION OF DOCUMENTARY MATE-
9 RIAL.—The production of documentary material in
10 response to a civil investigative demand shall be
11 made under a sworn certificate, in such form as the
12 demand designates, by the person, if a natural per-
13 son, to whom the demand is directed or, if not a
14 natural person, by any person having knowledge of
15 the facts and circumstances relating to such produc-
16 tion, to the effect that all of the documentary mate-
17 rial required by the demand and in the possession,
18 custody, or control of the person to whom the de-
19 mand is directed has been produced and made avail-
20 able to the custodian.

21 (11) SUBMISSION OF TANGIBLE THINGS.—The
22 submission of tangible things in response to a civil
23 investigative demand shall be made under a sworn
24 certificate, in such form as the demand designates,
25 by the person to whom the demand is directed or,

1 if not a natural person, by any person having knowl-
2 edge of the facts and circumstances relating to such
3 production, to the effect that all of the tangible
4 things required by the demand and in the posses-
5 sion, custody, or control of the person to whom the
6 demand is directed have been submitted to the cus-
7 todian.

8 (12) SEPARATE ANSWERS.—Each reporting re-
9 quirement or question in a civil investigative demand
10 shall be answered separately and fully in writing
11 under oath, unless it is objected to, in which event
12 the reasons for the objection shall be stated in lieu
13 of an answer, and it shall be submitted under a
14 sworn certificate, in such form as the demand des-
15 ignates, by the person, if a natural person, to whom
16 the demand is directed or, if not a natural person,
17 by any person responsible for answering each report-
18 ing requirement or question, to the effect that all in-
19 formation required by the demand and in the posses-
20 sion, custody, control, or knowledge of the person to
21 whom the demand is directed has been submitted.

22 (13) TESTIMONY.—

23 (A) IN GENERAL.—

24 (i) OATH AND RECORDATION.—The
25 examination of any person pursuant to a

1 demand for oral testimony served under
2 this subsection shall be taken before an of-
3 ficer authorized to administer oaths and
4 affirmations by the laws of the United
5 States or of the place at which the exam-
6 ination is held. The officer before whom
7 oral testimony is to be taken shall put the
8 witness on oath or affirmation and shall
9 personally, or by any individual acting
10 under the direction of and in the presence
11 of the officer, record the testimony of the
12 witness.

13 (ii) TRANSCRIPTION.—The testimony
14 shall be taken stenographically and tran-
15 scribed.

16 (B) PARTIES PRESENT.—Any Agency in-
17 vestigator before whom oral testimony is to be
18 taken shall exclude from the place where the
19 testimony is to be taken all other persons, ex-
20 cept the person giving the testimony, the attor-
21 ney for that person, the officer before whom the
22 testimony is to be taken, an investigator or rep-
23 resentative of an agency with which the Agency
24 is engaged in a joint investigation, and any ste-
25 nographer taking such testimony.

1 (C) LOCATION.—The oral testimony of any
2 person taken pursuant to a civil investigative
3 demand shall be taken in the judicial district of
4 the United States in which such person resides,
5 is found, or transacts business, or in such other
6 place as may be agreed upon by the Agency in-
7 vestigator before whom the oral testimony of
8 such person is to be taken and such person.

9 (D) ATTORNEY REPRESENTATION.—

10 (i) IN GENERAL.—Any person com-
11 pelled to appear under a civil investigative
12 demand for oral testimony pursuant to this
13 subsection may be accompanied, rep-
14 resented, and advised by an attorney.

15 (ii) AUTHORITY.—The attorney may
16 advise a person described in clause (i), in
17 confidence, either upon the request of such
18 person or upon the initiative of the attor-
19 ney, with respect to any question asked of
20 such person.

21 (iii) OBJECTIONS.—A person de-
22 scribed in clause (i), or the attorney for
23 that person, may object on the record to
24 any question, in whole or in part, and such
25 person shall briefly state for the record the

1 reason for the objection. An objection may
2 properly be made, received, and entered
3 upon the record when it is claimed that
4 such person is entitled to refuse to answer
5 the question on grounds of any constitu-
6 tional or other legal right or privilege, in-
7 cluding the privilege against self-incrimina-
8 tion, but such person shall not otherwise
9 object to or refuse to answer any question,
10 and such person or attorney shall not oth-
11 erwise interrupt the oral examination.

12 (iv) REFUSAL TO ANSWER.—If a per-
13 son described in clause (i) refuses to an-
14 swer any question—

15 (I) the Agency may petition the
16 district court of the United States
17 pursuant to this section for an order
18 compelling such person to answer
19 such question; and

20 (II) if the refusal is on grounds
21 of the privilege against self-incrimina-
22 tion, the testimony of such person
23 may be compelled in accordance with
24 the provisions of section 6004 of title
25 18, United States Code.

1 (E) TRANSCRIPTS.—For purposes of this
2 subsection—

3 (i) after the testimony of any witness
4 is fully transcribed, the Agency investi-
5 gator shall afford the witness (who may be
6 accompanied by an attorney) a reasonable
7 opportunity to examine the transcript;

8 (ii) the transcript shall be read to or
9 by the witness, unless such examination
10 and reading are waived by the witness;

11 (iii) any changes in form or substance
12 which the witness desires to make shall be
13 entered and identified upon the transcript
14 by the Agency investigator, with a state-
15 ment of the reasons given by the witness
16 for making such changes;

17 (iv) the transcript shall be signed by
18 the witness, unless the witness in writing
19 waives the signing, is ill, cannot be found,
20 or refuses to sign; and

21 (v) if the transcript is not signed by
22 the witness during the 30-day period fol-
23 lowing the date on which the witness is
24 first afforded a reasonable opportunity to
25 examine the transcript, the Agency investi-

1 gator shall sign the transcript and state on
2 the record the fact of the waiver, illness,
3 absence of the witness, or the refusal to
4 sign, together with any reasons given for
5 the failure to sign.

6 (F) CERTIFICATION BY INVESTIGATOR.—

7 The Agency investigator shall certify on the
8 transcript that the witness was duly sworn by
9 him or her and that the transcript is a true
10 record of the testimony given by the witness,
11 and the Agency investigator shall promptly de-
12 liver the transcript or send it by registered or
13 certified mail to the custodian.

14 (G) COPY OF TRANSCRIPT.—The Agency
15 investigator shall furnish a copy of the tran-
16 script (upon payment of reasonable charges for
17 the transcript) to the witness only, except that
18 the Agency may for good cause limit such wit-
19 ness to inspection of the official transcript of
20 his testimony.

21 (H) WITNESS FEES.—Any witness appear-
22 ing for the taking of oral testimony pursuant to
23 a civil investigative demand shall be entitled to
24 the same fees and mileage which are paid to

1 witnesses in the district courts of the United
2 States.

3 (d) CONFIDENTIAL TREATMENT OF DEMAND MATE-
4 RIAL.—

5 (1) IN GENERAL.—Documentary materials and
6 tangible things received as a result of a civil inves-
7 tigative demand shall be subject to requirements and
8 procedures regarding confidentiality, in accordance
9 with rules established by the Agency.

10 (2) DISCLOSURE TO CONGRESS.—No rule es-
11 tablished by the Agency regarding the confidentiality
12 of materials submitted to, or otherwise obtained by,
13 the Agency shall be intended to prevent disclosure to
14 either House of Congress or to an appropriate com-
15 mittee of the Congress, except that the Agency is
16 permitted to adopt rules allowing prior notice to any
17 party that owns or otherwise provided the material
18 to the Agency and had designated such material as
19 confidential.

20 (e) PETITION FOR ENFORCEMENT.—

21 (1) IN GENERAL.—Whenever any person fails
22 to comply with any civil investigative demand duly
23 served upon him under this section, or whenever sat-
24 isfactory copying or reproduction of material re-
25 quested pursuant to the demand cannot be accom-

1 plished and such person refuses to surrender such
2 material, the Agency, through such officers or attor-
3 neys as it may designate, may file, in the district
4 court of the United States for any judicial district
5 in which such person resides, is found, or transacts
6 business, and serve upon such person, a petition for
7 an order of such court for the enforcement of this
8 section.

9 (2) SERVICE OF PROCESS.—All process of any
10 court to which application may be made as provided
11 in this subsection may be served in any judicial dis-
12 trict.

13 (f) PETITION FOR ORDER MODIFYING OR SETTING
14 ASIDE DEMAND.—

15 (1) IN GENERAL.—Not later than 20 days after
16 the service of any civil investigative demand upon
17 any person under subsection (c), or at any time be-
18 fore the return date specified in the demand, which-
19 ever period is shorter, or within such period exceed-
20 ing 20 days after service or in excess of such return
21 date as may be prescribed in writing, subsequent to
22 service, by any Agency investigator named in the de-
23 mand, such person may file with the Agency a peti-
24 tion for an order by the Agency modifying or setting
25 aside the demand.

1 (2) COMPLIANCE DURING PENDENCY.—The
2 time permitted for compliance with the demand in
3 whole or in part, as determined proper and ordered
4 by the Agency, shall not run during the pendency of
5 a petition under paragraph (1) at the Agency, except
6 that such person shall comply with any portions of
7 the demand not sought to be modified or set aside.

8 (3) SPECIFIC GROUNDS.—A petition under
9 paragraph (1) shall specify each ground upon which
10 the petitioner relies in seeking relief, and may be
11 based upon any failure of the demand to comply
12 with the provisions of this section, or upon any con-
13 stitutional or other legal right or privilege of such
14 person.

15 (g) CUSTODIAL CONTROL.—At any time during
16 which any custodian is in custody or control of any docu-
17 mentary material, tangible things, reports, answers to
18 questions, or transcripts of oral testimony given by any
19 person in compliance with any civil investigative demand,
20 such person may file, in the district court of the United
21 States for the judicial district within which the office of
22 such custodian is situated, and serve upon such custodian,
23 a petition for an order of such court requiring the per-
24 formance by such custodian of any duty imposed upon him
25 by this section or rule promulgated by the Agency.

1 (h) JURISDICTION OF COURT.—

2 (1) IN GENERAL.—Whenever any petition is
3 filed in any district court of the United States under
4 this section, such court shall have jurisdiction to
5 hear and determine the matter so presented, and to
6 enter such order or orders as may be required to
7 carry out the provisions of this section.

8 (2) APPEAL.—Any final order entered as de-
9 scribed in paragraph (1) shall be subject to appeal
10 pursuant to section 1291 of title 28, United States
11 Code.

12 **SEC. 403. HEARINGS AND ADJUDICATION PROCEEDINGS.**

13 (a) IN GENERAL.—The Agency is authorized to con-
14 duct hearings and adjudication proceedings with respect
15 to any person in the manner prescribed by chapter 5 of
16 title 5, United States Code, in order to ensure or enforce
17 compliance with this division and the rules prescribed
18 under this division.

19 (b) SPECIAL RULES FOR CEASE-AND-DESIST PRO-
20 CEEDINGS.—

21 (1) ORDERS AUTHORIZED.—

22 (A) IN GENERAL.—If, in the opinion of the
23 Agency, a person is engaging or has engaged in
24 an act or omission that violates any provision of
25 this division or a rule or order prescribed under

1 this division, the Agency may issue and serve
2 upon the person a notice of charges in respect
3 thereof.

4 (B) CONTENT OF NOTICE.—The notice
5 under subparagraph (A) shall contain a state-
6 ment of the facts constituting the alleged viola-
7 tion, and shall fix a time and place at which a
8 hearing will be held to determine whether an
9 order to cease and desist should issue against
10 the person, such hearing to be held not earlier
11 than 30 days nor later than 60 days after the
12 date of service of such notice, unless an earlier
13 or a later date is set by the Agency, at the re-
14 quest of any person so served.

15 (C) CONSENT.—Unless a person served
16 under subparagraph (B) appears at the hearing
17 personally or by a duly authorized representa-
18 tive, the person shall be deemed to have con-
19 sented to the issuance of the cease-and-desist
20 order.

21 (D) PROCEDURE.—In the event of consent
22 under subparagraph (C), or if, upon the record
23 made at any such hearing, the Agency finds
24 that any violation specified in the notice of
25 charges has been established, the Agency may

1 issue and serve upon the person an order to
2 cease and desist from the violation. Such order
3 may, by provisions which may be mandatory or
4 otherwise, require the person to cease and de-
5 sist from the subject act or omission, and to
6 take affirmative action to correct the conditions
7 resulting from any such violation.

8 (2) EFFECTIVENESS OF ORDER.—A cease-and-
9 desist order shall become effective at the expiration
10 of 30 days after the date of service of the order
11 under paragraph (1)(D) (except in the case of a
12 cease-and-desist order issued upon consent, which
13 shall become effective at the time specified therein),
14 and shall remain effective and enforceable as pro-
15 vided therein, except to such extent as the order is
16 stayed, modified, terminated, or set aside by action
17 of the Agency or a reviewing court.

18 (3) DECISION AND APPEAL.—Any hearing pro-
19 vided for in this subsection shall be held in the Fed-
20 eral judicial district or in the territory in which the
21 residence or principal office or place of business of
22 the person is located unless the person consents to
23 another place, and shall be conducted in accordance
24 with the provisions of chapter 5 of title 5, United
25 States Code. After such hearing, and not later than

1 90 days after the Agency has notified each party to
2 the proceeding that the case has been submitted to
3 the Agency for final decision, the Agency shall
4 render its decision (which shall include findings of
5 fact upon which its decision is predicated) and shall
6 issue and serve upon each such party an order or or-
7 ders consistent with the provisions of this section.
8 Judicial review of any such order shall be exclusively
9 as provided in this subsection. Unless a petition for
10 review is timely filed in a court of appeals of the
11 United States, as provided in paragraph (4), and
12 thereafter until the record in the proceeding has
13 been filed as provided in paragraph (4), the Agency
14 may at any time, upon such notice and in such man-
15 ner as the Agency shall determine proper, modify,
16 terminate, or set aside any such order. Upon filing
17 of the record as provided, the Agency may modify,
18 terminate, or set aside any such order with permis-
19 sion of the court.

20 (4) APPEAL TO COURT OF APPEALS.—Any
21 party to any proceeding under this subsection may
22 obtain a review of any order served pursuant to this
23 subsection (other than an order issued with the con-
24 sent of the party) by filing in the court of appeals
25 of the United States for the circuit in which the resi-

1 dence or principal office or place of business of the
2 party is located, or in the United States Court of
3 Appeals for the District of Columbia Circuit, within
4 30 days after the date of service of such order, a
5 written petition praying that the order of the Agency
6 be modified, terminated, or set aside. A copy of such
7 petition shall be forthwith transmitted by the clerk
8 of the court to the Agency, and thereupon the Agen-
9 cy shall file in the court the record in the pro-
10 ceeding, as provided in section 2112 of title 28,
11 United States Code. Upon the filing of such petition,
12 such court shall have jurisdiction, which upon the
13 filing of the record shall, except as provided in the
14 last sentence of paragraph (3), be exclusive, to af-
15 firm, modify, terminate, or set aside, in whole or in
16 part, the order of the Agency. Review of such pro-
17 ceedings shall be had as provided in chapter 7 of
18 title 5, United States Code. The judgment and de-
19 cree of the court shall be final, except that the same
20 shall be subject to review by the Supreme Court of
21 the United States, upon certiorari, as provided in
22 section 1254 of title 28, United States Code.

23 (5) NO STAY.—The commencement of pro-
24 ceedings for judicial review under paragraph (4)

1 shall not, unless specifically ordered by the court,
2 operate as a stay of any order issued by the Agency.

3 (c) SPECIAL RULES FOR TEMPORARY CEASE-AND-
4 DESIST PROCEEDINGS.—

5 (1) IN GENERAL.—Whenever the Agency deter-
6 mines that the violation specified in the notice of
7 charges served upon a person pursuant to subsection
8 (b), or the continuation thereof, is likely to cause the
9 person to be insolvent or otherwise prejudice the in-
10 terests of individuals before the completion of the
11 proceedings conducted pursuant to subsection (b),
12 the Agency may issue a temporary order requiring
13 the person to cease and desist from any such viola-
14 tion and to take affirmative action to prevent or
15 remedy such insolvency or other condition pending
16 completion of such proceedings. Such order may in-
17 clude any requirement authorized under this title.
18 Such order shall become effective upon service upon
19 the person and, unless set aside, limited, or sus-
20 pended by a court in proceedings authorized by
21 paragraph (2), shall remain effective and enforceable
22 pending the completion of the administrative pro-
23 ceedings pursuant to such notice and until such time
24 as the Agency shall dismiss the charges specified in
25 such notice, or if a cease-and-desist order is issued

1 against the person, until the effective date of such
2 order.

3 (2) APPEAL.—Not later than 10 days after a
4 person has been served with a temporary cease-and-
5 desist order, the person may apply to the United
6 States district court for the judicial district in which
7 the residence or principal office or place of business
8 of the person is located, or the United States Dis-
9 trict Court for the District of Columbia, for an in-
10 junction setting aside, limiting, or suspending the
11 enforcement, operation, or effectiveness of such
12 order pending the completion of the administrative
13 proceedings pursuant to the notice of charges served
14 upon the person under subsection (b), and such
15 court shall have jurisdiction to issue such injunction.

16 (d) SPECIAL RULES FOR ENFORCEMENT OF OR-
17 DERS.—

18 (1) IN GENERAL.—The Agency may in its dis-
19 cretion apply to the United States district court
20 within the jurisdiction of which the residence or
21 principal office or place of business of a person is lo-
22 cated, for the enforcement of any effective and out-
23 standing order issued under this section against
24 such person, and such court shall have jurisdiction

1 and power to order and require compliance with
2 such order.

3 (2) EXCEPTION.—Except as otherwise provided
4 in this section, no court shall have jurisdiction to af-
5 fect by injunction or otherwise the issuance or en-
6 forcement of any order or to review, modify, sus-
7 pend, terminate, or set aside any such order.

8 (e) RULES.—The Agency shall prescribe rules estab-
9 lishing such procedures as may be necessary to carry out
10 this section.

11 **SEC. 404. LITIGATION AUTHORITY.**

12 (a) IN GENERAL.—If a person violates any provision
13 of this division or a rule or order prescribed under this
14 division, the Agency may commence a civil action against
15 such person to impose a civil penalty or to seek all appro-
16 priate legal and equitable relief, including a permanent or
17 temporary injunction.

18 (b) REPRESENTATION.—Except as provided in sub-
19 section (e), the Agency may act in its own name and
20 through its own attorneys in any action, suit, or other
21 court proceeding to which the Agency is a party.

22 (c) COMPROMISE OF ACTIONS.—The Agency may
23 compromise or settle any action, suit, or other court pro-
24 ceeding to which the Agency is a party if such compromise
25 is approved by the court.

1 (d) NOTICE TO THE ATTORNEY GENERAL.—

2 (1) IN GENERAL.—When commencing a civil
3 action under subsection (a), the Agency shall notify
4 the Attorney General.

5 (2) NOTICE AND COORDINATION.—

6 (A) NOTICE OF OTHER ACTIONS.—In addi-
7 tion to any notice required under paragraph
8 (1), the Agency shall notify the Attorney Gen-
9 eral concerning any action, suit, or other court
10 proceeding to which the Agency is a party.

11 (B) COORDINATION.—In order to avoid
12 conflicts and promote consistency regarding liti-
13 gation of matters under Federal law, the Attor-
14 ney General and the Agency shall consult re-
15 garding the coordination of investigations and
16 proceedings, including by negotiating an agree-
17 ment for coordination by not later than 180
18 days after the effective date specified in section
19 4(a). The agreement under this subparagraph
20 shall include provisions to ensure that parallel
21 investigations and proceedings involving this di-
22 vision and the rules prescribed under this divi-
23 sion are conducted in a manner that avoids con-
24 flicts and does not impede the ability of the At-

1 torney General to prosecute violations of Fed-
2 eral criminal laws.

3 (C) RULE OF CONSTRUCTION.—Nothing in
4 this paragraph shall be construed to limit the
5 authority of the Agency under this division, in-
6 cluding the authority to interpret this division.

7 (e) APPEARANCE BEFORE THE SUPREME COURT.—
8 The Agency may represent itself in its own name before
9 the Supreme Court of the United States, if the Agency
10 makes a written request to the Attorney General within
11 the 10-day period which begins on the date of entry of
12 the judgment which would permit any party to file a peti-
13 tion for writ of certiorari, and the Attorney General con-
14 curs with such request or fails to take action within 60
15 days of the request of the Agency.

16 (f) FORUM.—Any civil action brought under sub-
17 section (a) may be brought in an appropriate district court
18 of the United States or an appropriate State court.

19 (g) TIME FOR BRINGING ACTION.—Except as other-
20 wise permitted by law or equity, no action may be brought
21 under subsection (a) more than 3 years after the date of
22 discovery of the violation to which the action relates.

1 **SEC. 405. COORDINATION WITH OTHER FEDERAL AGEN-**
2 **CIES.**

3 (a) COORDINATION.—With respect to covered entities
4 and service providers, to the extent that Federal law au-
5 thorizes the Agency and another Federal agency to enforce
6 privacy laws, the other Federal agency shall coordinate
7 with the Agency to promote consistent enforcement of this
8 Act and other Federal privacy laws.

9 (b) REFERRAL.—Any Federal agency authorized to
10 enforce a Federal privacy law described in section 501
11 may recommend in writing to the Agency that the Agency
12 initiate an enforcement proceeding, as the Agency is au-
13 thorized by that Federal law or by this Act.

14 (c) COORDINATION WITH THE FEDERAL TRADE
15 COMMISSION.—

16 (1) IN GENERAL.—The Agency and the Federal
17 Trade Commission shall negotiate an agreement for
18 coordinating with respect to enforcement actions by
19 each agency regarding the provision of a product or
20 service offered by any covered entity. The agreement
21 shall include procedures for notice to the other agen-
22 cy, where feasible, prior to initiating a civil action to
23 enforce any Federal law regarding the privacy of in-
24 dividuals or security of personal information.

25 (2) CIVIL ACTIONS.—Whenever a civil action
26 has been filed by, or on behalf of, the Agency or the

1 Federal Trade Commission for any violation of any
2 provision of Federal law described in paragraph (1),
3 or any regulation prescribed under such provision of
4 law—

5 (A) the other agency may not, during the
6 pendency of that action, institute a civil action
7 under such provision of law against any defend-
8 ant named in the complaint in such pending ac-
9 tion for any violation alleged in the complaint;
10 and

11 (B) the Agency or the Federal Trade Com-
12 mission may intervene as a party in any such
13 action brought by the other agency, and, upon
14 intervening—

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

17 (ii) file petitions for appeal in such ac-
18 tions.

19 (3) AGREEMENT TERMS.—The terms of any
20 agreement negotiated under paragraph (1) may
21 modify or supersede the provisions of paragraph (2).

22 (4) DEADLINE.—The agencies shall reach the
23 agreement required under paragraph (1) not later
24 than 6 months after the designated transfer date.

1 **SEC. 406. ENFORCEMENT BY STATES.**

2 (a) CIVIL ACTION.—In any case in which the attor-
3 ney general of a State has reason to believe that an inter-
4 est of the residents of such State has been or is adversely
5 affected by any person who violates any provision of this
6 division or a rule or order prescribed under this division,
7 the attorney general of the State, as *parens patriae*, may
8 bring a civil action on behalf of the residents of the State
9 in an appropriate State court or an appropriate district
10 court of the United States—

11 (1) to enjoin further violation of such provision
12 by the defendant;

13 (2) to compel compliance with such provision;
14 or

15 (3) to obtain relief under section 408.

16 (b) RIGHTS OF AGENCY.—Before initiating a civil ac-
17 tion under subsection (a), the attorney general of a State
18 shall notify the Agency in writing of such civil action.
19 Upon receiving notice with respect to a civil action, the
20 Agency may—

21 (1) intervene in such action; and

22 (2) upon intervening—

23 (A) be heard on all matters arising in such
24 civil action; and

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

1 (c) **PREEMPTIVE ACTION BY AGENCY.**—If the Agen-
2 cy institutes a civil action for violation of any provision
3 of this division or a rule or order prescribed under this
4 division, no attorney general of a State may bring a civil
5 action against any defendant named in the complaint of
6 the Agency for a violation of such provision that is alleged
7 in such complaint.

8 **SEC. 407. PRIVATE RIGHTS OF ACTION.**

9 (a) **INJUNCTIVE RELIEF.**—A person who is aggrieved
10 by a violation of this division may bring a civil action for
11 declaratory or injunctive relief in any court of competent
12 jurisdiction in any State or in an appropriate district
13 court.

14 (b) **CIVIL ACTION FOR DAMAGES.**—Except for claims
15 under rule 23 of the Federal Rules of Civil Procedure or
16 a similar judicial procedure authorizing an action to be
17 brought by 1 or more representatives, a person who is ag-
18 grieved by a violation of this division may bring a civil
19 action for damages in any court of competent jurisdiction
20 in any State or in an appropriate district court.

21 (c) **NONPROFIT COLLECTIVE REPRESENTATION.**—
22 An individual shall have the right to appoint a nonprofit
23 body, organization, or association which has been properly
24 constituted in accordance with the law, has statutory ob-
25 jectives which are in the public interest, and is active in

1 the field of the protection of individual rights and free-
2 doms with regard to the protection of their personal data
3 to lodge the complaint on his or her behalf, to exercise
4 the rights referred to in this division on his or her behalf.

5 (1) A nonprofit may represent a class of ag-
6 grieved individuals.

7 (2) A prevailing nonprofit shall receive reason-
8 able compensation for expenses, including attorneys
9 fees.

10 (3) Individuals shall receive an equally divided
11 share of the total damages.

12 (d) STATE APPOINTMENT.—A State may provide
13 that any body, organization or association referred to in
14 subsection (c), independently of an individual's appoint-
15 ment, has the right to lodge, in that State, a complaint
16 with the Agency and to exercise the rights referred to in
17 this division if it considers that the rights of an individual
18 under this division have been infringed.

19 **SEC. 408. RELIEF AVAILABLE.**

20 (a) CIVIL ACTIONS AND ADJUDICATION PRO-
21 CEEDINGS.—

22 (1) JURISDICTION.—In any civil action or any
23 adjudication proceeding brought by the Agency or
24 the attorney general of a State, under any provision
25 of this division or a rule or order prescribed under

1 this division, the court or the Agency (as the case
2 may be) shall have jurisdiction to grant any appro-
3 priate legal or equitable relief with respect to a viola-
4 tion of such provision.

5 (2) RELIEF.—Relief under this section may in-
6 clude—

7 (A) rescission or reformation of contracts;

8 (B) refund of moneys;

9 (C) restitution;

10 (D) disgorgement or compensation for un-
11 just enrichment;

12 (E) payment of damages or other mone-
13 tary relief;

14 (F) public notification regarding the viola-
15 tion, including the costs of notification;

16 (G) limits on the activities or functions of
17 the person; and

18 (H) civil money penalties, as provided in
19 subsection (c).

20 (3) NO EXEMPLARY OR PUNITIVE DAMAGES.—

21 Nothing in this subsection shall be construed as au-
22 thorizing the imposition of exemplary or punitive
23 damages.

24 (b) RECOVERY OF COSTS.—In any civil action
25 brought by the Agency or the attorney general of a State

1 under any provision of this division or a rule or order pre-
2 scribed under this division, the Agency or attorney general
3 may recover its costs in connection with prosecuting such
4 action if the Agency or attorney general is the prevailing
5 party in the action.

6 (c) CIVIL MONEY PENALTY IN COURT AND ADJU-
7 DICATION PROCEEDINGS.—

8 (1) IN GENERAL.—Any person who violates,
9 through any act or omission, any provision of this
10 division or a rule or order prescribed under this divi-
11 sion shall forfeit and pay a civil penalty under this
12 subsection.

13 (2) PENALTY AMOUNT.—

14 (A) IN GENERAL.—The amount of a civil
15 penalty under this subsection may not exceed,
16 for each violation, the product of—

17 (i) the maximum civil penalty for
18 which a person, partnership, or corporation
19 may be liable under section 5(m)(1)(A) of
20 the Federal Trade Commission Act (15
21 U.S.C. 45(m)(1)(A)) for a violation of a
22 rule under such Act respecting unfair or
23 deceptive acts or practices, as adjusted
24 under the Federal Civil Penalties Inflation

1 Adjustment Act of 1990 (28 U.S.C. 2461
2 note); and

3 (ii) the number of individuals the per-
4 sonal information of which is affected by
5 the violation.

6 (B) CONTINUING VIOLATIONS.—In the
7 case of a violation through continuing failure to
8 comply with a provision of this division or a
9 rule or order prescribed under this division,
10 each day of continuance of such failure shall be
11 treated as a separate violation for purposes of
12 subparagraph (A).

13 (3) MITIGATING FACTORS.—In determining the
14 amount of any penalty assessed under paragraph
15 (2), the court or the Agency shall take into account
16 the appropriateness of the penalty with respect to—

17 (A) the size of financial resources and good
18 faith of the person charged;

19 (B) the gravity of the violation;

20 (C) the severity of the privacy harms (in-
21 cluding both actual and potential harms) to in-
22 dividuals;

23 (D) any disparate impact of the privacy
24 harms (including both actual and potential
25 harms) on protected classes;

1 (E) the history of previous violations; and
2 (F) such other matters as justice may re-
3 quire.

4 (4) AUTHORITY TO MODIFY OR REMIT PEN-
5 ALTY.—The Agency or attorney general of a State
6 may compromise, modify, or remit any penalty which
7 may be assessed or has already been assessed under
8 paragraph (2). The amount of such penalty, when fi-
9 nally determined, shall be exclusive of any sums
10 owed by the person to the United States in connec-
11 tion with the costs of the proceeding, and may be
12 deducted from any sums owing by the United States
13 to the person charged.

14 (5) NOTICE AND HEARING.—No civil penalty
15 may be assessed under this subsection with respect
16 to a violation of any provision of this division or a
17 rule or order prescribed under this division, unless—

18 (A) the Agency or attorney general of a
19 State gives notice and an opportunity for a
20 hearing to the person accused of the violation;
21 or

22 (B) the appropriate court has ordered such
23 assessment and entered judgment in favor of
24 the Agency or attorney general of a State.

1 **SEC. 409. REFERRAL FOR CRIMINAL PROCEEDINGS.**

2 If the Agency obtains evidence that any person, do-
3 mestic or foreign, has engaged in conduct that may con-
4 stitute a violation of Federal criminal law, the Agency
5 shall transmit such evidence to the Attorney General of
6 the United States, who may institute criminal proceedings
7 under appropriate law. Nothing in this section affects any
8 other authority of the Agency to disclose information.

9 **SEC. 410. WHISTLEBLOWER ENFORCEMENT.**

10 (a) IN GENERAL.—Any person who becomes aware,
11 based on non-public information, that a covered entity has
12 violated this division may file a civil action for civil pen-
13 alties, if prior to filing such action, the person files with
14 the Director a written request for the Director to com-
15 mence the action. The request shall include a clear and
16 concise statement of the grounds for believing a cause of
17 action exists. The person shall make the non-public infor-
18 mation available to the Director upon request:

19 (1) If the Director files suit within 90 days
20 from receipt of the written request to commence the
21 action, no other action may be brought unless the
22 action brought by the Director is dismissed without
23 prejudice.

24 (2) If the Director does not file suit within 90
25 days from receipt of the written request to com-

1 mence the action, the person requesting the action
2 may proceed to file a civil action.

3 (3) The time period within which a civil action
4 shall be commenced shall be tolled from the date of
5 receipt by the Director of the written request to ei-
6 ther the date that the civil action is dismissed with-
7 out prejudice, or for 150 days, whichever is later,
8 but only for a civil action brought by the person who
9 requested the Director to commence the action.

10 (b) ALLOCATION OF CIVIL PENALTIES.—If a judg-
11 ment is entered against the defendant or defendants in
12 an action brought pursuant to this section, or the matter
13 is settled, amounts received as civil penalties or pursuant
14 to a settlement of the action shall be allocated as follows:

15 (1) If the action was brought by the Director
16 upon a request made by a person pursuant to (a),
17 the person who made the request shall be entitled to
18 15 percent of the civil penalties.

19 (2) If the action was brought by the person who
20 made the request pursuant to (a), that person shall
21 receive an amount the court determines is reason-
22 able for collecting the civil penalties on behalf of the
23 government. The amount shall be not less than 25
24 percent and not more than 50 percent of the pro-

1 ceeds of the action and shall be paid out of the pro-
2 ceeds.

3 **TITLE V—RELATION TO OTHER**
4 **LAW**

5 **SEC. 501. RELATION TO OTHER FEDERAL LAW.**

6 Nothing in this division shall be construed to—

7 (1) modify, limit, or supersede the operation of
8 any privacy or security provision in—

9 (A) section 552a of title 5, United States
10 Code (commonly known as the “Privacy Act of
11 1974”);

12 (B) the Right to Financial Privacy Act of
13 1978 (12 U.S.C. 3401 et seq.);

14 (C) the Fair Credit Reporting Act (15
15 U.S.C. 1681 et seq.);

16 (D) the Fair Debt Collection Practices Act
17 (15 U.S.C. 1692 et seq.);

18 (E) the Children’s Online Privacy Protec-
19 tion Act of 1998 (15 U.S.C. 6501 et seq.);

20 (F) title V of the Gramm-Leach-Bliley Act
21 (15 U.S.C. 6801 et seq.);

22 (G) chapter 119, 123, or 206 of title 18,
23 United States Code;

24 (H) section 444 of the General Education
25 Provisions Act (20 U.S.C. 1232g) (commonly

1 referred to as the “Family Educational Rights
2 and Privacy Act of 1974”);

3 (I) section 445 of the General Education
4 Provisions Act (20 U.S.C. 1232h);

5 (J) the Privacy Protection Act of 1980 (42
6 U.S.C. 2000aa et seq.);

7 (K) the regulations promulgated under sec-
8 tion 264(e) of the Health Insurance Portability
9 and Accountability Act of 1996 (42 U.S.C.
10 1320d–2 note), as those regulations relate to—

11 (i) a person described in section
12 1172(a) of the Social Security Act (42
13 U.S.C. 1320d–1(a)); or

14 (ii) transactions referred to in section
15 1173(a)(1) of the Social Security Act (42
16 U.S.C. 1320d–2(a)(1));

17 (L) the Communications Assist-
18 ance for Law Enforcement Act (47
19 U.S.C. 1001 et seq.);

20 (M) section 222, 227, 338, or 631 of the
21 Communications Act of 1934 (47 U.S.C. 222,
22 227, 338, or 551);

23 (N) the E-Government Act of 2002 (44
24 U.S.C. 101 et seq.);

1 (O) the Paperwork Reduction Act of 1995
2 (44 U.S.C. 3501 et seq.);

3 (P) Federal Information Security Manage-
4 ment Act of 2002 (44 U.S.C. 3541 et seq.);

5 (Q) the Currency and Foreign Trans-
6 actions Reporting Act of 1970, as amended
7 (commonly known as the Bank Secrecy Act)
8 (12 U.S.C. 1829b and 1951–1959, 31 U.S.C.
9 5311–5314 and 5316–5332), including the
10 International Money Laundering Abatement
11 and Financial Anti-Terrorism Act of 2001, title
12 III of Public Law 107–56, as amended;

13 (R) the National Security Act of 1947 (50
14 U.S.C. 3001 et seq.);

15 (S) the Foreign Intelligence Surveillance
16 Act of 1978, as amended (50 U.S.C. 1801 et
17 seq.);

18 (T) the Civil Rights Act of 1964 (Public
19 Law 88–352, 78 Stat. 241);

20 (U) the Americans with Disabilities Act
21 (42 U.S.C. 12101 et seq.);

22 (V) the Fair Housing Act (42 U.S.C. 3601
23 et seq.);

1 (W) the Dodd-Frank Wall Street Reform
2 and Consumer Protection Act (Public Law
3 111–203, 124 Stat. 1376–2223);

4 (X) the Equal Credit Opportunity Act (15
5 U.S.C. 1691 et seq.);

6 (Y) the Age Discrimination in Employment
7 Act (29 U.S.C. 621 et seq.);

8 (Z) the Genetic Information Non-
9 discrimination Act (Public Law 110–233, 122
10 Stat. 881); or

11 (AA) any other privacy or security provi-
12 sion of Federal law; or

13 (2) limit the authority of the Federal Commu-
14 nications Commission to promulgate regulations and
15 enforce any privacy law not in contradiction with
16 this division.

17 **SEC. 502. SEVERABILITY.**

18 If any provision of this division, or the application
19 thereof, is held unconstitutional or otherwise invalid, the
20 validity of the remainder of the Act and the application
21 of such provision shall not be affected thereby.

