

116TH CONGRESS
1ST SESSION

H. R. 4978

To provide for individual rights relating to privacy of personal information, to establish privacy and security requirements for covered entities relating to personal information, and to establish an agency to be known as the United States Digital Privacy Agency to enforce such rights and requirements, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 5, 2019

Ms. ESHOO (for herself and Ms. LOFGREN) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committee on the Judiciary, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To provide for individual rights relating to privacy of personal information, to establish privacy and security requirements for covered entities relating to personal information, and to establish an agency to be known as the United States Digital Privacy Agency to enforce such rights and requirements, and for other purposes.

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

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

2 (a) SHORT TITLE.—This Act may be cited as the
3 “Online Privacy Act of 2019”.

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

- Sec. 1. Short title; table of contents.
- Sec. 2. Definitions.
- Sec. 3. Prohibition on waivers.
- Sec. 4. Effective date.
- Sec. 5. Journalism protection.
- Sec. 6. Small business compliance ramp.
- Sec. 7. Criminal prohibition on disclosing personal information.
- Sec. 8. 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. 2. DEFINITIONS.**

2 In this Act:

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

1 a period of time, or an aggregate of the per-
2 sonal information of one or more similarly situ-
3 ated individuals and designed to—

4 (i) alter, influence, guide, or predict
5 an individual’s behavior;

6 (ii) tailor or personalize a product or
7 service; or

8 (iii) filter, sort, limit, promote, display
9 or otherwise differentiate between specific
10 content or categories of content that would
11 otherwise be accessible to the individual.

12 (B) EXCLUSIONS.—The term “behavioral
13 personalization” does not include the use of his-
14 torical personal information to merely prevent
15 the display of or provide additional information
16 about previously accessed content.

17 (3) COLLECT.—The term “collect” includes,
18 with respect to personal information or contents of
19 communication, obtaining such information in any
20 manner, except when solely transmitting, routing,
21 providing intermediate storage for, or providing con-
22 nections for personal information through a system
23 or network.

24 (4) CONTENTS.—The term “contents”, when
25 used with respect to communication, has the mean-

1 ing given such term in section 2510 of title 18,
2 United States Code.

3 (5) COVERED ENTITY.—

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

6 (i) intentionally collects, processes, or
7 maintains personal information; and

8 (ii) sends or receives such personal in-
9 formation over the internet or a similar
10 communications network.

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

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

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

1 (A) a purpose specified by the covered en-
2 tity to the third party at the time of disclosure;
3 or

4 (B) a purpose to which the individual to
5 whom the information relates has consented.

6 (8) DE-Identified.—

7 (A) IN GENERAL.—The term “de-identi-
8 fied” means information that cannot reasonably
9 identify, relate to, describe, reference, be capa-
10 ble of being associated with, or be linked, di-
11 rectly or indirectly, to a particular individual or
12 device, provided that a business that uses de-
13 identified information—

14 (i) has de-identified the personal in-
15 formation using best practices for the
16 types of data the information contains;

17 (ii) has implemented technical safe-
18 guards that prohibit re-identification of the
19 individual with whom the information was
20 linked;

21 (iii) has implemented business proc-
22 esses that specifically prohibit re-identifica-
23 tion of the information;

1 (iv) has implemented business proc-
2 esses to prevent inadvertent release of de-
3 identified information; and

4 (v) makes no attempt to re-identify
5 the information.

6 (B) The Director may determine that a
7 methodology of de-identifying personal informa-
8 tion is insufficient for the purposes of this defi-
9 nition.

10 (9) DIRECTOR.—The term “Director” means
11 the Director of the Agency.

12 (10) DISCLOSE.—The term “disclose” means,
13 with respect to personal information or contents of
14 communication, to sell, release, transfer, share, dis-
15 seminate, make available, or otherwise cause to be
16 communicated such information to a third party.

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

20 (12) MAINTAIN.—The term “maintain” means,
21 with respect to personal information or contents of
22 communication, to store, secure, or otherwise cause
23 the retaining of such information, or taking actions
24 necessary for such purposes.

25 (13) PERSONAL INFORMATION.—

1 (A) IN GENERAL.—The term “personal in-
2 formation” means any information maintained
3 by a covered entity that is linked or reasonably
4 linkable to a specific individual or a specific de-
5 vice, including de-identified personal informa-
6 tion and the means to behavioral personaliza-
7 tion created for or linked to a specific indi-
8 vidual.

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

11 (i) publicly available information re-
12 lated to an individual; or

13 (ii) information derived or inferred
14 from personal information, if the derived
15 or inferred information is not linked or
16 reasonably linkable to a specific individual.

17 (14) PRIVACY HARM.—The term “privacy
18 harm” means adverse consequences or potential ad-
19 verse consequences to an individual or society arising
20 from the collection, processing, maintenance, or dis-
21 closure of personal information, including—

22 (A) direct or indirect financial loss or eco-
23 nomic harm;

24 (B) physical harm;

1 (C) psychological harm, including anxiety,
2 embarrassment, fear, and other demonstrable
3 mental trauma;

4 (D) adverse outcomes or decisions with re-
5 spect to the eligibility of an individual for
6 rights, benefits, or privileges in employment (in-
7 cluding hiring, firing, promotion, demotion, and
8 compensation), credit and insurance (including
9 denial of an application or obtaining less favor-
10 able terms), housing, education, professional
11 certification, or the provision of health care and
12 related services;

13 (E) stigmatization or reputational harm;

14 (F) price discrimination;

15 (G) other adverse consequences that affect
16 the private life of an individual, including pri-
17 vate family matters and actions and commu-
18 nications within the home of such individual or
19 a similar physical, online, or digital location
20 where such individual has a reasonable expecta-
21 tion that personal information will not be col-
22 lected, processed, or retained;

23 (H) chilling of free expression or action of
24 an individual, group of individuals, or society
25 generally, due to perceived or actual pervasive

1 and excessive collection, processing, disclosure,
2 or maintenance of personal information by a
3 covered entity;

4 (I) impairing the autonomy of an indi-
5 vidual, group of individuals, or society gen-
6 erally; and

7 (J) other adverse consequences or potential
8 adverse consequences, consistent with the provi-
9 sions of this Act, as determined by the Direc-
10 tor.

11 (15) PRIVACY PRESERVING COMPUTING.—

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

14 (i) the collecting, processing, dis-
15 closing, or maintaining of personal infor-
16 mation that has been encrypted or other-
17 wise rendered unintelligible using a means
18 that cannot be reversed by a covered enti-
19 ty, or a covered entity’s service provider,
20 such that—

21 (I) if such personal information
22 could be rendered intelligible through
23 cooperation or sharing of cryp-
24 tographic secrets by multiple persons,
25 the covered entity has both technical

1 safeguards and business processes to
2 prevent such cooperation or sharing;

3 (II) if such personal information
4 is rendered intelligible within a hard-
5 ware processing unit or other means
6 of performing operations on the infor-
7 mation, there are technical safeguards
8 that, during the normal course of op-
9 eration—

10 (aa) prevent rendering per-
11 sonal information intelligible any-
12 where but within the hardware
13 processing unit or other means of
14 performing operations; and

15 (bb) make the exporting or
16 otherwise observing of such intel-
17 ligible information, or the cryp-
18 tographic secret used to protect
19 such information, impossible; and

20 (III) if the result of such proc-
21 essing of the personal information is
22 also personal information, such result
23 must be unintelligible to the covered
24 entity or service provider and pro-

1 tected by privacy preserving com-
2 puting.

3 (B) INSUFFICIENT METHODOLOGIES.—The
4 Director may determine that a methodology of
5 privacy preserving computing is insufficient for
6 the purposes of this definition.

7 (16) PROCESS.—The term “process” means to
8 perform or cause to be performed any operation or
9 set of operations on personal information or contents
10 of communication, whether or not by automated
11 means.

12 (17) PROTECTED CLASS.—The term “protected
13 class” means the actual or perceived race, color, eth-
14 nicity, national origin, religion, sex (including sexual
15 orientation and gender identity), familial status, or
16 disability of an individual or group of individuals.

17 (18) PUBLICLY AVAILABLE INFORMATION.—
18 The term “publicly available information” means—

19 (A) information that is lawfully made
20 available from Federal, State, or local govern-
21 ment records;

22 (B) information about a public individual
23 or official that is made publicly accessible, with-
24 out restrictions on accessibility other than the

1 general authorization to access the services used
2 to make the information accessible;

3 (C) information made publicly accessible
4 by the individual to whom it pertains, without
5 restrictions on accessibility other than the gen-
6 eral authorization to access the services used to
7 make the information accessible, and that such
8 individual has the ability to delete or change
9 without relying on a request under section 102
10 or 103 of this Act; and

11 (D) does not include—

12 (i) biometric information collected by
13 a covered entity relating to an individual
14 without the individual's knowledge;

15 (ii) information used for a purpose
16 that is not compatible with the purpose for
17 which the information is maintained and
18 made available in government records;

19 (iii) information obtained from gov-
20 ernment records for the purpose of selling
21 such information; or

22 (iv) information used to contact or lo-
23 cate a private individual either physically
24 or electronically.

1 (19) REASONABLE MECHANISM.—The term
2 “reasonable mechanism” means, in the case of a
3 mechanism for individuals to exercise a right under
4 title I or interact with a covered entity under title
5 II, that such mechanism—

6 (A) is equivalent in availability and ease of
7 use to that of other mechanisms for commu-
8 nicating or interacting with the covered entity;
9 and

10 (B) includes an online means of exercising
11 such right or engaging in such interaction, if
12 such individuals communicate or interact with
13 such covered entity through an online medium
14 or if such covered entity provides information
15 processing services through a public or widely
16 available application programming interface (or
17 similar mechanism).

18 (20) SELL AND SALE.—

19 (A) IN GENERAL.—The terms “sell” and
20 “sale” means the disclosure of personal infor-
21 mation for monetary consideration by a covered
22 entity to a third party for the purposes of proc-
23 essing, maintaining or disclosing such personal
24 information at the third party’s discretion.

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

3 (i) the disclosure of personal data to
4 a third party with which the individual has
5 a direct relationship for purposes of pro-
6 viding a product or service requested by
7 the individual or otherwise in a manner
8 that is consistent with an individual’s rea-
9 sonable expectations considering the con-
10 text in which the individual provided the
11 personal information to the covered entity;

12 (ii) the disclosure or transfer of per-
13 sonal information to a subsidiary or an af-
14 filiate of the covered entity; or

15 (iii) the disclosure or transfer of per-
16 sonal information to a third party as an
17 asset that is part of a merger, acquisition,
18 bankruptcy, or other transaction in which
19 the third party assumes control of all or
20 part of the covered entity’s assets, unless
21 such assets are limited to personal infor-
22 mation unless personal information makes
23 up the majority of the value of such assets.

24 (21) SERVICE PROVIDER.—

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

3 (i) processes, discloses, or maintains
4 personal information, where such person
5 does not process, disclose, or maintain the
6 personal information other than in accord-
7 ance with the directions and on behalf of
8 another covered entity;

9 (ii) does not directly collect personal
10 information from or control the mechanism
11 for collecting personal information from an
12 individual;

13 (iii) does not earn revenue from proc-
14 essing, maintaining, or disclosing personal
15 information disclosed to the service pro-
16 vider by a covered entity except by pro-
17 viding contracted services to another cov-
18 ered entity;

19 (iv) does not disclose personal infor-
20 mation to another covered entity unless it
21 was provided by that covered entity or re-
22 sulted from maintaining or processing per-
23 formed on personal information exclusively
24 provide by that covered entity;

1 (v) does not offer services that allow
2 another covered entity to target specific in-
3 dividuals using personal information not
4 provided by that covered entity;

5 (vi) assists a covered entity on behalf
6 of which it processes personal information
7 to comply with title I, with respect to per-
8 sonal information processed or maintained
9 by the service provider on behalf of the
10 covered entity, including providing tools for
11 such covered entities requirements under
12 title I if requested; and

13 (vii) does not link the personal infor-
14 mation provided by another covered entity
15 to personal information from any other
16 source.

17 (B) Any such person, and the personal in-
18 formation they disclose, process, or maintain,
19 shall be treated as a service provider under this
20 Act only to the extent that such person com-
21 plies with the requirements under (A).

22 (22) SIGNIFICANT PRIVACY HARM.—The term
23 “significant privacy harm” means adverse con-
24 sequences to an individual arising from the collec-
25 tion, processing, maintenance, or disclosure of per-

1 sonal information, limited to subparagraph (A), (B),
2 or (D) of paragraph (14).

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

5 (A) does not earn revenue from the sale of
6 personal information;

7 (B) earns less than half of annual revenues
8 from the processing of personal information for
9 targeted or personalized advertising;

10 (C) has not, at any time during the pre-
11 ceding 6-month period, maintained personal in-
12 formation of 250,000 or more individuals;

13 (D) has fewer than 200 employees; and

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

17 (24) STATE.—The term “State” means each
18 State of the United States, the District of Columbia,
19 each commonwealth, territory, or possession of the
20 United States, and each federally recognized Indian
21 Tribe.

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

24 (A) to whom such covered entity disclosed
25 personal information; and

- 1 (B) is not—
- 2 (i) such covered entity;
- 3 (ii) a subsidiary or corporate affiliate
- 4 of such covered entity; or
- 5 (iii) a service provider of such covered
- 6 entity.

7 **SEC. 3. PROHIBITION ON WAIVERS.**

8 (a) IN GENERAL.—The provisions under this Act

9 may not be waived. Any agreement purporting to waive

10 compliance with or modify any provision of this Act shall

11 be void as contrary to public policy.

12 (b) PROHIBITION ON PREDISPUTE ARBITRATION

13 AGREEMENTS.—No predispute arbitration agreement

14 shall be valid or enforceable with respect to any claims

15 under this Act.

16 **SEC. 4. EFFECTIVE DATE.**

17 (a) IN GENERAL.—This Act shall apply beginning on

18 the date that is 1 year after the date of the enactment

19 of this Act.

20 (b) AUTHORITY TO PROMULGATE REGULATIONS AND

21 TAKE CERTAIN OTHER ACTIONS.—Nothing in subsection

22 (a) affects the authority to take an action expressly re-

23 quired by a provision of this Act to be taken before the

24 effective date described in such subsection.

1 **SEC. 5. JOURNALISM PROTECTION.**

2 (a) IN GENERAL.—Covered entities engaged in jour-
3 nalism shall not be subject to the obligations imposed
4 under this Act to the extent that those obligations directly
5 infringe on the journalism rather than the business prac-
6 tices of the covered entity, so long as, the covered entity
7 has technical safeguards and business processes that pre-
8 vent the collection, processing, maintaining, or disclosure
9 of such personal information for business practices other
10 than journalism.

11 (b) JOURNALISM.—The term “journalism” includes
12 the collecting, maintaining, processing, and disclosing of
13 personal information about a public individual or official,
14 or that otherwise concerns matters of public interest, for
15 dissemination to the public.

16 **SEC. 6. SMALL BUSINESS COMPLIANCE RAMP.**

17 Upon losing its status as a small business, a covered
18 entity shall have nine months to comply with provisions
19 of this Act that a small business is exempt from complying
20 with.

21 **SEC. 7. CRIMINAL PROHIBITION ON DISCLOSING PER-**
22 **SONAL INFORMATION.**

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

1 **“§ 881. Disclosure of personal information with the**
2 **intent to cause harm**

3 “Whoever uses a channel of interstate or foreign com-
4 merce to knowingly disclose an individual’s personal infor-
5 mation—

6 “(1) with the intent to threaten, intimidate, or
7 harass any person, incite or facilitate the commis-
8 sion of a crime of violence against any person, or
9 place any person in reasonable fear of death or seri-
10 ous bodily injury; or

11 “(2) with the intent that the information will be
12 used to threaten, intimidate, or harass any person,
13 incite or facilitate the commission of a crime of vio-
14 lence against any person, or place any person in rea-
15 sonable fear of death or serious bodily injury,

16 shall be fined under this title or imprisoned not more than
17 5 years, or both.”.

18 **SEC. 8. LIMITATION ON DISCLOSING NONREDACTED GOV-**
19 **ERNMENT RECORDS.**

20 (a) IN GENERAL.—A Federal or State government
21 entity may not use a channel of interstate commerce to
22 disclose the personal information of an individual in a gov-
23 ernment record without an agreement prohibiting the re-
24 cipient of such information from selling the information
25 without the express consent of the individual for each dis-
26 closure.

1 (b) EXCEPTION.—Notwithstanding subsection (a),
2 nothing in this section shall prohibit the disclosure of per-
3 sonal information using a channel of interstate commerce
4 to another government entity without consent of the indi-
5 vidual.

6 **TITLE I—INDIVIDUAL RIGHTS**

7 **SEC. 101. RIGHT OF ACCESS.**

8 (a) IN GENERAL.—A covered entity shall make avail-
9 able a reasonable mechanism by which an individual may
10 access—

11 (1) the categories of personal information and
12 contents of communications of such individual that
13 is maintained by such covered entity, including, in
14 the case of personal information that such covered
15 entity did not collect from such individual, how and
16 from whom such covered entity obtained such per-
17 sonal information;

18 (2) a list of the third parties, subsidiaries, and
19 corporate affiliates, to which such covered entity has
20 disclosed and from which such covered entity has, at
21 any time on or after the effective date specified in
22 section 4(a), obtained the personal information of
23 such individual;

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

4 (A) for collecting, processing, or maintain-
5 ing the personal information of such individual;
6 and

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

9 (4) a list of automated decision-making proc-
10 esses that an individual has a right to request
11 human review of under section 105 with a concise
12 and clear description of the implications and in-
13 tended effects of such process.

14 (b) EXCEPTION FOR PUBLICLY ACCESSIBLY INFOR-
15 MATION.—A covered entity that makes available informa-
16 tion required in subsection (a) shall be considered in com-
17 pliance with such requirements if the covered entity pro-
18 vides an individual instructions on how to access a public
19 posting of such information, including in a privacy policy,
20 if the instructions are easy and do not require payment.

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

23 **SEC. 102. RIGHT OF CORRECTION.**

24 (a) DISPUTE BY INDIVIDUAL.—A covered entity shall
25 make available a reasonable mechanism by which an indi-

1 individual may dispute the accuracy or completeness of per-
2 sonal information linked to such individual that is main-
3 tained by such covered entity if such information is proc-
4 essed in any way, by such covered entity, a third party
5 of such covered entity, or a service provider of such cov-
6 ered entity that may increase reasonably foreseeable sig-
7 nificant privacy harms.

8 (b) CORRECTION BY COVERED ENTITY.—A covered
9 entity receiving a dispute under subsection (a) shall—

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

13 (2) notify such individual that—

14 (A) the disputed information is correct or
15 complete;

16 (B) such covered entity lacks sufficient in-
17 formation to correct or complete the disputed
18 information; or

19 (C) such covered entity is denying the re-
20 quest for correction or completion in reliance on
21 an exemption or exception provided by section
22 109(g) (with the notification containing an
23 identification of the specific exemption or excep-
24 tion relied upon).

1 (c) SMALL BUSINESSES EXCLUDED.—This section
2 does not apply to a small business.

3 **SEC. 103. RIGHT OF DELETION.**

4 (a) REQUEST BY INDIVIDUAL.—A covered entity
5 shall make available a reasonable mechanism by which an
6 individual may request the deletion of personal informa-
7 tion and contents of communications of such individual
8 maintained by such covered entity, including any such in-
9 formation that such covered entity acquired from a third
10 party or inferred from other information maintained by
11 such covered entity.

12 (b) DELETION BY COVERED ENTITY.—A covered en-
13 tity receiving a request for deletion under subsection (a)
14 shall—

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

17 (2) notify such individual that such covered en-
18 tity is denying the request for deletion in reliance on
19 an exemption or exception provided by section
20 109(g) (with the notification containing an identi-
21 fication of the specific exemption or exception relied
22 upon).

23 **SEC. 104. RIGHT OF PORTABILITY.**

24 (a) DETERMINATION OF PORTABLE CATEGORIES.—

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

3 (A) establish categories of products and
4 services offered by covered entities, based on
5 similarities in the products and services;

6 (B) determine which categories established
7 under subparagraph (A) are portable categories;
8 and

9 (C) publish in the Federal Register a list
10 of portable categories determined under sub-
11 paragraph (B).

12 (2) OPPORTUNITY FOR PUBLIC COMMENT.—Be-
13 fore publishing the final list under paragraph (1)(C),
14 the Director shall—

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

17 (B) provide for an opportunity for public
18 comment on such draft list.

19 (b) EXERCISE OF RIGHT.—

20 (1) IN GENERAL.—A covered entity that offers
21 a product or service in a portable category shall
22 make available to an individual whose personal infor-
23 mation or contents of communications such entity
24 maintains a reasonable mechanism by which such in-
25 dividual may—

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

3 (i) any personal information of such
4 individual that such individual has pro-
5 vided to such covered entity, with the op-
6 tion to download such information by cat-
7 egory that is accessible under section 101
8 of this Act; and

9 (ii) any contents of communications;
10 and

11 (B) using a real-time application program-
12 ming interface, or similar mechanism, transmit
13 all personal information and contents of com-
14 munications of or related to such individual
15 (whether or not provided to such covered entity
16 by such individual) from such covered entity to
17 another covered entity in accordance with sub-
18 section (c).

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

23 (A) be publicly documented;

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

1 (C) include a publicly available, fully func-
2 tional test version for development purposes;
3 and

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

6 (c) REQUIREMENTS FOR ACCESS TO APPLICATION
7 PROGRAMMING INTERFACE.—

8 (1) ACCESS.—A covered entity shall provide ac-
9 cess to the application programming interface or
10 similar mechanism required by subsection (b)(1)(B)
11 upon the request of another covered entity if the re-
12 questing covered entity has self-certified, using the
13 procedures established by the Director under para-
14 graph (3)(A), that such requesting covered entity—

15 (A) is a covered entity;

16 (B) can have personal information dis-
17 closed to it under section 205 of this Act;

18 (C) is, at the time of the self-certification,
19 in compliance with all requirements of this Act
20 (including provisions a small business is other-
21 wise exempt from complying with);

22 (D) will continue to comply with all re-
23 quirements of this Act; and

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

4 (2) DENIAL OF ACCESS.—

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

12 (B) REVIEW.—In accordance with the pro-
13 cedures established under paragraph (3)(B), a
14 covered entity the request of which is denied
15 under subparagraph (A) may petition the Di-
16 rector for review of the denial. If the Director
17 finds that such denial is unreasonable, the Di-
18 rector may impose a penalty, to be established
19 in such procedures, on the covered entity that
20 denied the request.

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

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

1 (B) procedures for the review of petitions
2 under paragraph (2)(B), including penalties for
3 unreasonable denials.

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

6 (e) DEFINITIONS.—In this section:

7 (1) PORTABLE CATEGORY.—The term “portable
8 category” means a category of products and services
9 established by the Director under subsection
10 (a)(1)(A)—

11 (A) for which the sum obtained by adding
12 the number of users or estimated users of each
13 product or service in such category is greater
14 than 10,000,000; and

15 (B) that—

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

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

21 (iii) the Director otherwise determines
22 that a category would benefit from encour-
23 aging increased competition.

24 (2) USERS.—The term “users” means, with re-
25 spect to a product or service, the monthly active

1 users, subscribers, or customers (or a reasonable
2 proxy or substitute therefor determined by the Di-
3 rector) of such product or service.

4 **SEC. 105. RIGHT TO HUMAN REVIEW OF AUTOMATED DECI-**
5 **SIONS.**

6 For any decision by a covered entity based solely on
7 automated processing of personal information of an indi-
8 vidual, if such processing increases reasonably foreseeable
9 significant privacy harms for such individual, such covered
10 entity shall—

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

13 (2) make available a reasonable mechanism by
14 which such individual may request human review of
15 such decision; and

16 (3) if such individual requests such a review,
17 conduct such review within a reasonable amount of
18 time after such request.

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

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

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

24 (2) process with; or

25 (3) otherwise link an individual with;

1 an algorithm, model, or other means designed for behav-
2 ioral personalization, without the affirmative express con-
3 sent of that individual.

4 (b) CONSENT.—A covered entity must obtain express
5 affirmative consent from an individual before it may pro-
6 vide a behaviorally personalized version of a product or
7 service. Where consent is denied, a covered entity must
8 provide the product or service without behavioral personal-
9 ization.

10 (c) EXCEPTIONS TO PROVIDING PRODUCT OR SERV-
11 ICE.—

12 (1) Where the offering of a substantially similar
13 product or service without behavioral personalization
14 is infeasible, a covered entity shall provide, to the
15 greatest extent feasible, a core aspect or part of the
16 product or service that can be offered without behav-
17 ioral personalization.

18 (2) Where no core aspect or part of the product
19 or service can function in a substantially similar
20 function without behavioral personalization, a cov-
21 ered entity may deny providing an individual use of
22 such product or service if such individual does not
23 consent to behavioral personalization as required in
24 subsection (a).

1 (d) EXCEPTION TO BEHAVIORAL PROCESSING.—Not-
2 withstanding subsections (a) and (b), a covered entity may
3 create or process using behavioral personalization algo-
4 rithms, models, or other mechanisms for the purpose of
5 increasing the usability of the product or service provided
6 by a covered entity that—

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

10 (2) have an output that is both uniform across
11 the individuals that use the product or service and
12 independent of a specific individual’s inherent or be-
13 havioral characteristics.

14 (e) USABILITY.—The term “usability” as used in
15 subsection (d) does not include optimizations or other al-
16 terations to the product or service that are made with the
17 primary purpose of increasing the amount of time an indi-
18 vidual engages with or uses the product or service, unless
19 such increase benefits the individual

20 (f) SMALL BUSINESSES EXCLUDED.—This section
21 does not apply to a small business.

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

23 A covered entity that collects personal information of
24 an individual with whom such covered entity does not have
25 an existing relationship (as of the time of the collection),

1 if such personal information includes contact information,
2 shall notify such individual within 30 days, in writing if
3 possible and at no charge to the individual, that such cov-
4 ered entity has collected the personal information of such
5 individual.

6 **SEC. 108. RIGHT TO IMPERMANENCE.**

7 (a) LIMITATION ON MAINTENANCE OF PERSONAL IN-
8 FORMATION.—A covered entity shall not maintain per-
9 sonal information for more time than expressly consented
10 to by an individual whose personal information is being
11 maintained.

12 (b) CONSENT.—A covered entity must obtain express
13 affirmative consent from an individual before maintaining
14 the personal information of such individual for any dura-
15 tion. Such consent may be obtained for categories of per-
16 sonal information and shall give an individual options to
17 affirmatively choose granting a covered entity consent for
18 various durations, at least including—

19 (1) for no longer than needed to complete the
20 specific request or transaction (including a reason-
21 able estimate of such duration by the covered enti-
22 ty);

23 (2) until consent is revoked; and

24 (3) one or more additional durations based on
25 reasonable expectations and norms for the mainte-

1 nance of the category of personal information being
2 maintained.

3 (c) EXCEPTION FOR IMPLIED CONSENT.—Where the
4 long-term maintenance of personal information is, on its
5 face, obvious and a core feature of the product or service
6 at the request of the individual, and the personal informa-
7 tion is maintained only to provide such product or service,
8 subsections (a) and (b) shall not apply.

9 **SEC. 109. EXEMPTIONS, EXCEPTIONS, FEES, TIMELINES,**
10 **AND RULES OF CONSTRUCTION FOR RIGHTS**
11 **UNDER THIS TITLE.**

12 (a) EXEMPTIONS FOR PERSONAL INFORMATION FOR
13 PARTICULAR PURPOSES.—

14 (1) IN GENERAL.—This title does not apply
15 with respect to personal information that is col-
16 lected, processed, maintained, or disclosed for any of
17 the following purposes (or a combination of such
18 purposes), where a covered entity has technical safe-
19 guards and business processes that limit the collec-
20 tion, processing, maintaining, or disclosure of such
21 personal information to the following purposes:

22 (A) Detecting, responding to, or preventing
23 security incidents or threats.

24 (B) Protecting against malicious, decep-
25 tive, fraudulent, or illegal activity.

1 (C) Complying with specific law enforce-
2 ment requests or court orders.

3 (D) Protecting a legally recognized privi-
4 lege or other legal right.

5 (E) Protecting public safety.

6 (F) Collection, processing, or maintenance
7 by an employer pursuant to an employer-em-
8 ployee relationship of records about employees
9 or employment status, except—

10 (i) where the information would not
11 be reasonably expected to be collected in
12 the context of an employee's regular du-
13 ties; or

14 (ii) was disclosed to the employer by
15 a third party.

16 (G) Preventing prospective abuses of a
17 service by an individual whose account has been
18 previously terminated.

19 (H) Routing a communication through a
20 communications network or resolving the loca-
21 tion of a host or client on a communications
22 network.

23 (I) Providing transparency in advertising
24 or origination of user generated content.

1 (2) REIDENTIFICATION.—Where compliance
2 with this title would require the reidentification of
3 de-identified personal information, and the covered
4 entity does not already maintain the information
5 necessary for such reidentification, the covered enti-
6 ty shall be exempt from such compliance, except for
7 with section 106.

8 (3) DISCLOSURE.—A covered entity relying on
9 an exemption under paragraph (1) with respect to
10 personal information shall disclose in the privacy
11 policy maintained by such entity under section
12 213—

13 (A) the reason for which such information
14 is collected, processed, maintained, or disclosed;
15 and

16 (B) a description of the rights provided by
17 this title that are not available with respect to
18 such personal information by reason of such ex-
19 emption.

20 (b) EXCEPTIONS FOR PARTICULAR REQUESTS.—

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

23 (A) such covered entity cannot confirm the
24 identity of such individual;

1 (B) such covered entity determines that
2 granting the request of such individual would
3 create a legitimate risk to the privacy, security,
4 safety, or other rights of another individual;

5 (C) such covered entity determines that
6 granting the request of such individual would
7 create a legitimate risk to free expression; or

8 (D) the personal information requested to
9 be corrected under section 102 or deleted under
10 section 103—

11 (i) is necessary to the completion of a
12 transaction initiated before such request
13 was made or the performance of a contract
14 entered into before such request was made;

15 (ii) was collected specifically for the
16 completion of such transaction or the per-
17 formance of such contract; and

18 (iii) would undermine the integrity of
19 a legally significant transaction.

20 (2) LIMITATIONS ON REQUESTS FOR ADDI-
21 TIONAL INFORMATION TO CONFIRM IDENTITY.—A
22 covered entity may not deny a request of an indi-
23 vidual under paragraph (1)(A) on the basis of the
24 refusal of such individual to provide additional per-

1 sonal information to such covered entity to confirm
2 the identity of such individual—

3 (A) if the identity of such individual can
4 reasonably be confirmed using personal infor-
5 mation of such individual that such covered en-
6 tity (as of the time of the request) already
7 maintains; or

8 (B) if such individual has an existing rela-
9 tionship (as of the time of the request) with
10 such covered entity, such individual has con-
11 firmed the identity of such individual to such
12 covered entity in the same manner as for other
13 transactions of a similar sensitivity.

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

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

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

24 (1) comply with such request; or

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

4 (f) FEES PROHIBITED.—

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

8 (2) UNFOUNDED OR EXCESSIVE REQUESTS.—If
9 a request under this title is unfounded or excessive,
10 a covered entity may charge a reasonable fee that
11 reflects the estimated administrative costs of com-
12 plying with such request.

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

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

19 (A) such fee to be unreasonable relative to
20 reasonable administrative costs of complying
21 with a request under this title; or

22 (B) such request is not unfounded or ex-
23 cessive.

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

1 (1) take an action that would convert informa-
2 tion that is not personal information into personal
3 information;

4 (2) collect or maintain personal information or
5 contents of communication that the covered entity
6 would otherwise not maintain; or

7 (3) maintain personal information or contents
8 of communication longer than the covered entity
9 would otherwise maintain such personal information.

10 (h) REGULATIONS.—The Director shall promulgate
11 regulations to implement this section.

12 **TITLE II—REQUIREMENTS FOR**
13 **COVERED ENTITIES, SERVICE**
14 **PROVIDERS, AND THIRD PAR-**
15 **TIES**

16 **SEC. 201. MINIMIZATION AND ARTICULATED BASIS FOR**
17 **COLLECTION, PROCESSING, AND MAINTEN-**
18 **NANCE.**

19 (a) ARTICULATED BASIS.—A covered entity shall
20 have a reasonable, articulated basis for the collection,
21 processing, disclosure, and maintenance of personal infor-
22 mation that takes into account the reasonable business
23 needs of the covered entity and minimum amount of per-
24 sonal information necessary for providing the service, bal-
25 anced with the intrusion on the privacy of, potential pri-

1 vacy harms to, and reasonable expectations of individuals
2 to whom the personal information relates.

3 (b) MINIMIZATION OF COLLECTION, PROCESSING,
4 DISCLOSURE, AND MAINTENANCE.—

5 (1) COLLECTION.—A covered entity may not
6 collect more personal information than is reasonably
7 needed to provide a product or service that an indi-
8 vidual has requested.

9 (2) PROCESSING.—A covered entity may not
10 process personal information for a purpose other
11 than the purpose for which such information was
12 originally collected from the individual or in the case
13 of a service provider, a purpose other than that
14 which is in accordance with the directions of a cov-
15 ered entity.

16 (3) DISCLOSURE.—A covered entity may not
17 disclose personal information for a purpose other
18 than the purpose for which such information was
19 originally collected from the individual or in the case
20 of a service provider, a purpose other than that
21 which is in accordance with the directions of a cov-
22 ered entity.

23 (4) MAINTENANCE.—A covered entity may not
24 maintain personal information once such information
25 is no longer needed for the purpose for which such

1 information was originally collected from the indi-
2 vidual or in the case of a service provider, a purpose
3 other than that which is in accordance with the di-
4 rections of a covered entity.

5 (c) ANCILLARY COLLECTION, PROCESSING, DISCLO-
6 SURE, AND MAINTENANCE.—Notwithstanding subsection
7 (b), a covered entity may engage in collection, processing,
8 disclosure, or maintenance of personal information beyond
9 limitations under subsection (b) only if such covered entity
10 complies with this subsection.

11 (1) NO NOTICE OR CONSENT REQUIRED.—A
12 covered entity may engage in collection, processing,
13 or maintenance of personal information without ad-
14 ditional notice or consent if the purpose for such col-
15 lection, processing, or maintenance is substantially
16 similar to the type of personal information and pur-
17 pose for which such personal information was origi-
18 nally collected and such ancillary collection, proc-
19 essing, or maintenance will not result in additional
20 or increased privacy harms.

21 (2) NOTICE REQUIRED.—A covered entity shall
22 provide notice of ancillary collection, processing, dis-
23 closure or maintenance of personal information in
24 the case of one, but not more than one, of the fol-
25 lowing:

1 (A) Such ancillary collection, processing,
2 disclosure, or maintenance may result in addi-
3 tional or increased privacy harms (but not in-
4 creased significant privacy harms), and is sub-
5 stantially similar to the purpose for which such
6 personal information was originally collected.

7 (B) The purpose for such ancillary collec-
8 tion, processing, disclosure, or maintenance is
9 not substantially similar to the purpose for
10 which such personal information was originally
11 collected, but will not result in additional or in-
12 creased privacy harms.

13 (C) Such ancillary collection, processing,
14 disclosure, or maintenance may result in addi-
15 tional or increased privacy harms (but not in-
16 creased significant privacy harms) and the pur-
17 pose is not substantially similar to the purpose
18 for which such personal information was origi-
19 nally collected, so long as, the personal informa-
20 tion is secured using privacy preserving com-
21 puting.

22 (3) NOTICE AND CONSENT REQUIRED.—For
23 scenarios not covered under paragraph (1) or (2),
24 and notwithstanding section 212(b)(2) and (3), a
25 covered entity shall provide notice of and obtain con-

1 sent for ancillary collection, processing, disclosure or
2 maintenance of personal information.

3 (d) SUBSTITUTION.—In cases in which personal in-
4 formation can be replaced with artificial personal informa-
5 tion, personal information that has been de-identified, or
6 the random personal information of a one or more individ-
7 uals without substantially reducing the utility of the data
8 or requiring an unreasonable amount of effort, such a re-
9 placement shall take place.

10 **SEC. 202. MINIMIZATION AND RECORDS OF ACCESS BY EM-**
11 **PLOYEES AND CONTRACTORS.**

12 (a) MINIMIZATION.—A covered entity shall restrict
13 access to personal information and contents of commu-
14 nications by the employees or contractors of such covered
15 entity based on an articulated balance between the poten-
16 tial for privacy harm, reasonable expectations of individ-
17 uals to whom the personal information relates, and reason-
18 able business needs.

19 (b) RECORDS OF ACCESS.—

20 (1) IN GENERAL.—A covered entity shall main-
21 tain records identifying each instance in which an
22 employee or a contractor of such covered entity ac-
23 cesses personal information or contents of commu-
24 nications if disclosure of, or a data breach or data
25 sharing abuse involving, such personal information

1 or contents may foreseeably result in increased pri-
2 vacy harms.

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

5 (A) A unique identifier for the employee or
6 contractor accessing personal information or
7 contents of communications.

8 (B) The date and time of access.

9 (C) The fields of information accessed.

10 (D) The individuals whose personal infor-
11 mation was accessed or the contents of whose
12 communications were accessed.

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

15 **SEC. 203. PROHIBITION ON THE COLLECTION OR MAINTE-**
16 **NANCE OF PERSONAL INFORMATION.**

17 A covered entity may not collect or maintain personal
18 information using a channel of interstate commerce unless
19 such covered entity is in compliance with all requirements
20 of this Act.

21 **SEC. 204. PROHIBITIONS ON THE DISCLOSURE OF PER-**
22 **SONAL INFORMATION.**

23 (a) CONSENT FOR DISCLOSURE REQUIRED.—

24 (1) IN GENERAL.—A covered entity may not in-
25 tentiously disclose personal information unless the

1 covered entity obtains consent of the individual
2 whose personal information is being disclosed for
3 each category of third party to which such personal
4 information will be disclosed. Such covered entity
5 must also provide such individual with notice of—

6 (A) each category of third party;

7 (B) the personal information to be dis-
8 closed; and

9 (C) a concise and clear description of the
10 business or commercial purpose for such disclo-
11 sure.

12 (2) ADDITIONAL REQUIREMENTS FOR SALE OF
13 PERSONAL INFORMATION.—

14 (A) IN GENERAL.—A covered entity may
15 not intentionally sell personal information un-
16 less the covered entity—

17 (i) obtains the consent required by
18 paragraph (1) for each individual disclo-
19 sure of such person information; and

20 (ii) and provides the individual to
21 whom such personal information relates
22 with the identity of the specific third party
23 to which such personal information will be
24 disclosed.

1 (B) DISCLOSURE SERVICES.—Subpara-
2 graph (A) shall not apply to a covered entity in
3 a case in which an individual is directing the
4 covered entity to disclose the personal informa-
5 tion of such individual for the sole purpose of
6 procuring goods or services, or offers for goods
7 or services, for such individual, if there is a rea-
8 sonable mechanism for the individual to with-
9 draw consent.

10 (3) REQUIREMENT TO INCLUDE ORIGINAL PUR-
11 POSE OF COLLECTION.—A covered entity may not
12 intentionally disclose personal information without
13 including the purpose for which the personal infor-
14 mation was originally collected.

15 (4) EXCEPTION FOR PRIVACY PRESERVING
16 COMPUTING.—Notwithstanding paragraph (1), con-
17 sent is not required for a disclosure (not including
18 sale) of personal information secured using privacy
19 preserving computing.

20 (5) EXCEPTION FOR DE-IDENTIFIED PERSONAL
21 INFORMATION.—Notwithstanding paragraph (1),
22 consent is not required for a disclosure (not includ-
23 ing sale) of de-identified personal information where
24 the disclosed personal information is limited to the
25 narrowest possible scope likely to yield the intended

1 benefit and contractual obligations are in place that
2 prohibit—

3 (A) re-identification of the disclosed per-
4 sonal information; and

5 (B) the processing of additional personal
6 information in combination with the disclosed
7 personal information that would allow for the
8 reidentification of the disclosed personal infor-
9 mation.

10 (b) DISCLOSURE FOR ADVERTISING OR MARKETING
11 PURPOSES.—

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

18 (2) TREATMENT OF CERTAIN TYPES OF INFOR-
19 MATION.—A disclosure for advertising or marketing
20 purposes may not be treated as violating subpara-
21 graph (1) by reason of including any or all of the
22 following:

23 (A) Internet Protocol addresses truncated
24 to no more than the first 24 bits for Internet
25 Protocol version 4 and the first 48 bits for

1 Internet Protocol version 6, or for a successor
2 protocol truncated to limit the precision of the
3 identifier to a network address of the internet
4 access provider.

5 (B) Geolocation information truncated to
6 allow no more than the equivalent of two dec-
7 imal degrees of precision at the equator or
8 prime meridian, or an equivalent precision in
9 another geolocation standard.

10 (C) A general description of a device,
11 browser, or operating system, or any combina-
12 tion thereof.

13 (D) An identifier that is unique for each
14 disclosure.

15 **SEC. 205. DISCLOSURE TO ENTITIES NOT SUBJECT TO**
16 **UNITED STATES JURISDICTION OR NOT COM-**
17 **PLIANT WITH THIS ACT.**

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

20 (1) is not subject to the jurisdiction of the
21 United States; or

22 (2) is not in compliance with all requirements
23 of this Act.

24 (b) EXCEPTION.—Notwithstanding subsection (a), a
25 covered entity may disclose personal information where

1 that personal information is limited to an identifier cre-
2 ated primarily for the purpose of sending or receiving elec-
3 tronic communications and the sole purpose of the disclo-
4 sure is to send or receive an electronic communication at
5 the request of the individual whose personal information
6 is being disclosed.

7 (c) DISCLOSURE SAFE HARBORS.—Notwithstanding
8 subsection (a), a covered entity may disclose personal in-
9 formation to another covered entity (the receiving covered
10 entity) that is not subject to the jurisdiction of the United
11 States if either—

12 (1) the receiving covered entity has entered into
13 an agreement, as described in subsection (e), with
14 the Agency, and—

15 (A) the covered entity has a reasonable be-
16 lief that the receiving covered entity is suffi-
17 ciently solvent to compensate victims or pay
18 fines for violations of this Act;

19 (B) a contract between the covered entity
20 and receiving covered entity requires that the
21 receiving covered entity complies with this Act,
22 and the covered entity has reason to believe the
23 receiving covered entity is compliant with this
24 Act; and

1 (C) a contract between the covered entity
2 and the receiving covered entity prohibits the
3 receiving covered entity from using the dis-
4 closed personal information for any purpose
5 other than provided in the contract; or

6 (2) the covered entity has—

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

9 (i) requires the receiving covered enti-
10 ty to comply with this Act;

11 (ii) prohibits the receiving covered en-
12 tity from using the disclosed personal in-
13 formation for any purpose other than pro-
14 vided in the contract;

15 (iii) requires the receiving covered en-
16 tity to indemnify the covered entity against
17 violations of this Act committed by the re-
18 ceiving covered entity for any amount the
19 covered entity is unable to pay of a judg-
20 ment for such violation;

21 (iv) grants the covered entity the au-
22 thority to audit, including physical access
23 to electronic devices and data, the receiving
24 covered entity's compliance with this Act
25 and the contract; and

1 (v) requires the receiving covered enti-
2 ty to assist the covered entity in respond-
3 ing to and complying with any court or-
4 ders, Agency orders, or the exercising of
5 an individual's rights under this Act;

6 (B) actual knowledge that the receiving
7 covered entity is in compliance with this Act
8 and not using personal information contrary to
9 their agreement;

10 (C) actual knowledge that the receiving
11 covered entity is sufficiently solvent to com-
12 pensate victims or pay fines for violations of
13 this Act;

14 (D) an auditing and compliance program
15 to ensure the receiving covered entity's contin-
16 ued compliance with this Act and contract
17 terms;

18 (E) filed with the Agency the terms of said
19 contract, proof of its actual knowledge of the
20 receiving covered entity's compliance with this
21 Act and contract terms, and documents detail-
22 ing its auditing and compliance program for ap-
23 proval and publication by the Agency; and

24 (F) the covered entity has entered into an
25 agreement with the Agency where it agrees to

1 accept, respond to, or comply with a court
2 order, agency order, or request by an individual
3 regarding actions taken by the receiving covered
4 entity with respect to the data it has disclosed.

5 (d) For the purposes of subsection (c)(2), the covered
6 entity shall be jointly liable for a violation of this Act by
7 the receiving covered entity regarding the data the covered
8 entity disclosed, except where the covered entity was the
9 first to notify the Agency of the violation, in which case,
10 it shall be severally liable. Where the covered entity should
11 reasonably have known of a violation of this Act by the
12 receiving covered entity and fails to disclose the violation
13 to the Agency, each day of continuance of the failure to
14 report such violation shall be treated as a separate viola-
15 tion.

16 (e) AGENCY AGREEMENTS.—Upon the request of a
17 covered entity not subject to the jurisdiction of the United
18 States, the Agency shall enter into an agreement with the
19 covered entity that includes, but is not limited to, the fol-
20 lowing conditions:

21 (1) The principle place of business for the cov-
22 ered entity must be in a country that allows for the
23 domestication of a United States court decision for
24 civil fines payable to a government entity and in-
25 junctive relief. Where a foreign court refuses to en-

1 force a United States court decision under this Act,
2 the agreement, and all other agreements with cov-
3 ered entities with a principle place of business in the
4 same jurisdiction, shall be void.

5 (2) The covered entity agrees to comply with
6 this Act.

7 (3) The covered entity agrees to be subject to
8 this Act with choice of venue being a United States
9 court.

10 (4) The covered entity agrees to comply with
11 Agency investigative requests or orders, and United
12 States court orders or decisions under this Act.

13 (5) The covered entity consents to United
14 States Federal court personal jurisdiction for the
15 sole purpose of enforcing this Act.

16 (6) Where enforcement of the decision requires
17 the use of a foreign court, the covered entity agrees
18 to pay reasonable attorney fees necessary to enforce
19 the judgment.

20 (7) A default judgment, failure to comply with
21 Agency investigative requests or orders, or failure to
22 comply with United States court orders or decisions
23 shall result in the immediate termination of the
24 agreement.

1 (f) **RULE OF CONSTRUCTION AGAINST DATA LOCAL-**
2 **IZATION.**—Nothing in this section shall be construed to
3 require the localization of processing or maintaining per-
4 sonal information by a covered entity to within the United
5 State, or limit internal disclosure of personal information
6 within a covered entity or to subsidiary or corporate affil-
7 iate of such covered entity, regardless of the country in
8 which the covered entity will process, disclose, or maintain
9 that personal information.

10 **SEC. 206. PROHIBITION ON REIDENTIFICATION.**

11 (a) **IN GENERAL.**—Except as required under title I,
12 a covered entity shall not use personal information col-
13 lected from an individual, acquired from a third party, or
14 acquired from a publicly available information to reiden-
15 tify an individual from de-identified information.

16 (b) **THIRD-PARTY PROHIBITION.**—A covered entity
17 that discloses de-identified information to a third party
18 shall prohibit such third party from reidentifying an indi-
19 vidual using such de-identified information.

20 (c) **EXCEPTION.**—Subsection (a) shall not apply to
21 qualified research entities, as determined by the Director,
22 conducting research not for commercial purposes.

1 **SEC. 207. RESTRICTIONS ON COLLECTION, PROCESSING,**
2 **AND DISCLOSURE OF CONTENTS OF COMMU-**
3 **NICATIONS.**

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

9 (1) transmission or display of the communica-
10 tion to any intended recipient or the original sender,
11 or maintenance of such communications for such
12 purposes;

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

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

17 (4) processing expressly requested by the sender
18 or intended recipient, if the sender or intended re-
19 cipient can terminate such processing using a rea-
20 sonable mechanism;

21 (5) a disclosure otherwise required by law;

22 (6) the filtering of a communication where pri-
23 mary purpose of the communication is the commer-
24 cial advertisement or promotion of a commercial
25 product or service; or

1 (7) detecting or enforcing an abuse or violation
2 of the service’s terms of service that would result in
3 either a temporary or permanent ban from using the
4 service.

5 (b) INTENDED RECIPIENT.—A covered entity is not
6 considered an intended recipient of a communication, or
7 any communication used in the creation of the content of
8 said communication, where—

9 (1) at least one intended recipient is a natural
10 person other than an employee or contractor of the
11 covered entity;

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

14 (3) a purpose of the covered entity’s service is
15 to maintain, at the direction of the sender, the con-
16 tent of said communication for more than a transi-
17 tory period.

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

21 (1) Where the sender is a natural person, they
22 shall be the sender of the entire content of the com-
23 munication, regardless of the original author of any
24 portion of the content.

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

4 (d) EXCEPTION FOR PUBLICLY AVAILABLE COMMU-
5 NICATIONS.—Subsection (a) shall not apply where the con-
6 tents of communication that are made publicly accessible
7 by the sender without restrictions on accessibility other
8 than the general authorization to access the services used
9 to make the information accessible.

10 (e) ENCRYPTION PROTECTION.—A covered entity
11 shall not—

12 (1) prohibit or prevent a person from
13 encrypting or otherwise rendering unintelligible the
14 content of a communication using a means that pre-
15 vents the covered entity from being able to decrypt
16 or otherwise render intelligible said content; and

17 (2) require or cause a person to disclose or cir-
18 cumvent the means described in paragraph (1) to
19 the covered entity that would allow it to render the
20 content intelligible.

21 (f) SERVICE PROVIDERS SAFE HARBOR.—A service
22 provider shall not be held liable for a violation of this sec-
23 tion if such service provider is acting at the direction of
24 and on behalf of a covered entity and has a reasonable

1 belief that the covered entity's directions are in compliance
2 with this section.

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

4 (a) DISCRIMINATION IN ECONOMIC OPPORTUNI-
5 TIES.—A covered entity shall not process personal infor-
6 mation or contents of communication for advertising, mar-
7 keting, soliciting, offering, selling, leasing, licensing, rent-
8 ing, or otherwise commercially contracting for employ-
9 ment, finance, healthcare, credit, insurance, housing, or
10 education opportunities in a manner that discriminates
11 against or otherwise makes opportunities unavailable on
12 the basis of an individual's protected class status.

13 (b) PUBLIC ACCOMMODATIONS.—A covered entity
14 shall not process personal information in a manner that
15 segregates, discriminates in, or otherwise makes unavail-
16 able the goods, services, facilities, privileges, advantages,
17 or accommodations of any place of public accommodation
18 on the basis of a person's or a group's protected class sta-
19 tus.

20 (c) The Director shall promulgate regulations to im-
21 plement this section.

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

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

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

4 (2) research and services related to medical,
5 historical, or population uses of genetic information,
6 if, in the case of disclosure of genetic information—

7 (A) such genetic information is only dis-
8 closed to qualified research entities, as deter-
9 mined by the Director;

10 (B) additional personal information dis-
11 closed with such genetic information is limited
12 to the narrowest possible scope likely to yield
13 the intended benefit; and

14 (C) the covered entity limits, through con-
15 tractual obligations, additional types of personal
16 information that can be processed with the dis-
17 closed genetic information and personal infor-
18 mation.

19 (3) a purpose specified by the Director by regu-
20 lation, taking into account the potential privacy
21 harms and potential benefits of such collection, proc-
22 essing, maintenance, or disclosure; or

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

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

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

11 **SEC. 210. REQUIREMENTS FOR NOTICE AND CONSENT**
12 **PROCESSES AND PRIVACY POLICIES.**

13 (a) MINIMUM THRESHOLD.—The Director shall es-
14 tablish a minimum threshold that a covered entity must
15 meet for the percentage of individuals who read and un-
16 derstand a notice or consent process or privacy policy re-
17 quired by this Act. In establishing such minimum thresh-
18 olds, the Director shall take into account expectations of
19 individuals, potential privacy harms, and individuals’
20 awareness of privacy harms.

21 (b) CONSENT REVOCATION.—A covered entity shall
22 make available a reasonable mechanism by which an indi-
23 vidual may revoke consent for any consent given under
24 this Act.

25 (c) SAFE HARBOR.—

1 (1) APPROVAL PROCEDURES.—The Director
2 shall develop procedures for analyzing and approving
3 data submitted by a covered entity to establish that
4 a notice and consent process or privacy policy of
5 such covered entity meets the threshold established
6 under subsection (a).

7 (2) PRESUMPTION.—If a covered entity submits
8 testing data to and receives an approval from the
9 Director under paragraph (1) establishing that a no-
10 tice or consent process or privacy policy of such cov-
11 ered entity meets the threshold established under
12 subsection (a), such notice or consent process or pri-
13 vacy policy shall be presumed to have met such
14 threshold. Such presumption may be rebutted by
15 clear and convincing evidence.

16 (3) PUBLIC AVAILABILITY OF APPROVED PROC-
17 ESSES AND POLICIES AND ASSOCIATED TESTING
18 DATA.—The Director shall make publicly available
19 online the notice and consent processes and privacy
20 policies and associated testing data that the Director
21 approves under paragraph (1).

22 (4) SMALL BUSINESS ADOPTION OF NOTICE OR
23 CONSENT PROCESS OF ANOTHER COVERED ENTI-
24 TY.—

1 (A) IN GENERAL.—If a small business
2 adopts a notice or consent process of another
3 covered entity that collects, processes, main-
4 tains, or discloses personal information in sub-
5 stantially the same way as such small business,
6 if the process of such other covered entity has
7 been approved under paragraph (1), the process
8 of such small business shall receive the pre-
9 sumption under paragraph (2).

10 (B) ABILITY TO FREELY USE APPROVED
11 PROCESS.—A covered entity whose notice or
12 consent process is approved under paragraph
13 (1) shall permit a small business to freely use
14 such process, or a derivative thereof, as de-
15 scribed in subparagraph (A).

16 (C) NO PUBLISHED PROCESS.—In the case
17 of a small business for which there is no ap-
18 proved notice or consent process published
19 under paragraph (3) of a covered entity that
20 collects, processes, maintains, or discloses per-
21 sonal information in substantially the same way
22 as such small business, any requirement under
23 this title for a notice or consent process to be
24 objectively shown to meet the threshold estab-
25 lished by the Director under subsection (a)

1 shall not apply to such small business. Nothing
2 in the preceding sentence exempts a small busi-
3 ness from the requirement to use such notice or
4 consent process or that such process be concise
5 and clear.

6 (D) INAPPLICABILITY TO PRIVACY POL-
7 ICY.—Paragraph (4) does not apply with re-
8 spect to a privacy policy.

9 (5) MINOR CHANGES.—A covered entity may
10 make minor changes in a notice or consent process
11 or privacy policy approved under paragraph (1) and
12 retain the presumption under paragraph (2) for such
13 process or policy without retesting or resubmission
14 of testing data to the Director.

15 **SEC. 211. PROHIBITION ON DECEPTIVE NOTICE AND CON-**
16 **SENT PROCESSES AND PRIVACY POLICIES.**

17 In providing notice, obtaining consent, or maintaining
18 a privacy policy as required by this title, a covered entity
19 may not intentionally take any action that substantially
20 impairs, obscures, or subverts the ability of an individual
21 to—

22 (1) understand the contents of such notice or
23 such privacy policy;

24 (2) understand the process for granting such
25 consent;

1 (3) make a decision regarding whether to grant
2 or withdraw such consent; or

3 (4) act on any such decision.

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

5 (a) NOTICE.—A covered entity shall provide an indi-
6 vidual with notice of the personal information such covered
7 entity collects, processes, maintains, and discloses through
8 a process that is concise and clear and can be objectively
9 shown to meet the threshold established by the Director
10 under section 210(a).

11 (b) CONSENT.—

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

24 (2) EXCEPTION FOR IMPLIED CONSENT.—Not-
25 withstanding paragraph (1), express consent is not

1 required for collection, processing, or maintenance of
2 personal information if the collection, processing, or
3 maintenance is, on its face, obvious and necessary to
4 provide a service at the request of the individual and
5 the personal information is collected, processed, or
6 maintained only for such request. Nothing in this
7 paragraph shall be construed to exempt the covered
8 entity from the requirement of subsection (a) to pro-
9 vide notice to such individual with respect to such
10 collection, processing, or maintenance.

11 (3) EXEMPTION FOR PRIVACY PRESERVING
12 COMPUTING.—Notwithstanding paragraph (1), ex-
13 cept with regard to consent for purposes of section
14 106, express consent is not required for collection,
15 processing, or maintenance of personal information
16 secured using privacy preserving computing. Nothing
17 in this paragraph shall be construed to exempt the
18 covered entity from the requirement of subsection
19 (a) to provide notice to such individual with respect
20 to such collection, processing, or maintenance.

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

1 **SEC. 213. PRIVACY POLICY.**

2 (a) **POLICY REQUIRED.**—A covered entity shall main-
3 tain a privacy policy relating to the practices of such entity
4 regarding the collection, processing, maintenance, and dis-
5 closure of personal information.

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

8 (1) A general description of the practices of the
9 covered entity regarding the collection, processing,
10 maintenance, and disclosure of personal information.

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

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

15 (A) The categories of personal information
16 collected or otherwise obtained by the covered
17 entity.

18 (B) The business or commercial purposes
19 of the covered entity for collecting, processing,
20 maintaining, or disclosing personal information.

21 (C) The categories and a list of third par-
22 ties to which the covered entity discloses per-
23 sonal information.

24 (4) A description of the personal information
25 that the covered entity maintains that the covered

1 entity does not collect from individuals and how the
2 covered entity obtains such personal information.

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

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

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

12 (c) EXEMPTION FOR PERSONAL INFORMATION FOR
13 PARTICULAR PURPOSES.—The privacy policy required by
14 subsection (a) is not required to contain information relat-
15 ing to personal information that is collected, processed,
16 maintained, or disclosed exclusively for any of the pur-
17 poses described in paragraph (1) of section 109(a) (or a
18 combination of such purposes), except as provided in para-
19 graph (2) of such section.

20 (d) AVAILABILITY OF PRIVACY POLICY.—

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

23 (A) clear and in plain language; and

24 (B) made publicly available in a prominent
25 location on an ongoing basis.

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

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

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

13 **SEC. 214. INFORMATION SECURITY REQUIREMENTS.**

14 (a) **IN GENERAL.**—A covered entity shall establish
15 and implement reasonable information security policies,
16 practices, and procedures for the protection of personal
17 information collected, processed, maintained, or disclosed
18 by such covered entity, taking into consideration—

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

21 (2) the sensitivity of any personal information
22 at issue;

23 (3) the current state of the art in administra-
24 tive, technical, and physical safeguards for pro-
25 tecting such information; and

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

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

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

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

18 (2) A process for identifying and assessing rea-
19 sonably foreseeable security vulnerabilities in the
20 system or systems used by such covered entity that
21 contain personal information, which shall include
22 regular monitoring for vulnerabilities or data
23 breaches involving such system or systems.

24 (3) A process for taking action designed to
25 mitigate against vulnerabilities identified in the

1 process required by paragraph (2), which may in-
2 clude implementing any changes to security practices
3 and the architecture, installation, or implementation
4 of network or operating software, or for regularly
5 testing or otherwise monitoring the effectiveness of
6 the existing safeguards.

7 (4) A process for determining if personal infor-
8 mation is no longer needed and disposing of personal
9 information by shredding, permanently erasing, or
10 otherwise modifying the medium on which such per-
11 sonal information is maintained to make such per-
12 sonal information permanently unreadable or indeci-
13 pherable.

14 (5) A process for overseeing persons who have
15 access to personal information, including through
16 network-connected devices.

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

20 (7) A written plan or protocol for internal and
21 public response in the event of a data breach or data
22 sharing abuse.

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

1 (e) SMALL BUSINESSES ASSISTANCE.—The Director,
2 in consultation with the National Institute of Standards
3 and Technology, the Small Business Association, and
4 small businesses, shall develop policy templates, toolkits,
5 tip sheets, configuration guidelines for commonly used
6 hardware and software, interactive tools, and other mate-
7 rials to assist small businesses with complying with this
8 section.

9 **SEC. 215. NOTIFICATION OF DATA BREACH OR DATA SHAR-**
10 **ING ABUSE.**

11 (a) NOTIFICATION OF AGENCY.—

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

22 (2) REASONS FOR DELAY.—If the notification
23 required by paragraph (1) is made more than 72
24 hours after the covered entity becomes aware of the
25 data breach or data sharing abuse, such notification

1 shall be accompanied by a statement of the reasons
2 for the delay.

3 (b) NOTIFICATION OF OTHER COVERED ENTITY.—

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

22 (c) NOTIFICATION OF INDIVIDUALS.—

23 (1) IN GENERAL.—In the case of a data breach
24 or data sharing abuse with respect to personal infor-
25 mation maintained by a covered entity (or a data

1 breach or data sharing abuse about which a covered
2 entity is notified under subsection (b)), if such cov-
3 ered entity has a relationship with an individual
4 whose personal information was involved or poten-
5 tially involved in such data breach or data sharing
6 abuse, such covered entity shall notify such indi-
7 vidual of such data breach or data sharing abuse not
8 later than 14 days after becoming aware of such
9 data breach or data sharing abuse (or, in the case
10 of a data breach or data sharing abuse about which
11 a covered entity is notified under subsection (b), not
12 later than 14 days after being so notified), if such
13 data breach or data sharing abuse creates or in-
14 creases foreseeable privacy harms.

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

18 (A) the same medium through which such
19 individual routinely interacts with such covered
20 entity; and

21 (B) one additional medium of notification,
22 if such covered entity has the personal informa-
23 tion necessary to make a notification through
24 such an additional medium without causing ex-
25 cessive financial burden for such covered entity.

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

5 **TITLE III—UNITED STATES**
6 **DIGITAL PRIVACY AGENCY**

7 **SEC. 301. ESTABLISHMENT.**

8 (a) AGENCY ESTABLISHED.—There is established an
9 independent agency in the executive branch to be known
10 as the “United States Digital Privacy Agency”, which
11 shall implement and enforce this Act.

12 (b) DIRECTOR AND DEPUTY DIRECTOR.—

13 (1) IN GENERAL.—There is established the po-
14 sition of the Director, who shall serve as the head
15 of the Agency.

16 (2) APPOINTMENT.—Subject to paragraph (3),
17 the Director shall be appointed by the President, by
18 and with the advice and consent of the Senate.

19 (3) QUALIFICATION.—The President shall
20 nominate the Director from among individuals who
21 are citizens of the United States.

22 (4) DEPUTY DIRECTOR.—There is established
23 the position of Deputy Director, who shall—

24 (A) be appointed by the Director; and

1 (B) serve as acting Director in the absence
2 or unavailability of the Director.

3 (c) TERM.—

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

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

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

13 (d) SERVICE RESTRICTION.—No Director or Deputy
14 Director may hold any office, position, or employment in
15 any covered entity during the period of service of such per-
16 son as Director or Deputy Director.

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

21 (f) COMPENSATION.—

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

1 (2) CONFORMING AMENDMENT.—Section 5313
2 of title 5, United States Code, is amended by insert-
3 ing after the item relating to “Federal Transit Ad-
4 ministrators.” the following new item: “Director of
5 the United States Digital Privacy Agency.”.

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

7 (a) POWERS OF THE AGENCY.—The Director is au-
8 thorized to establish the general policies of the Agency
9 with respect to all executive and administrative functions,
10 including—

11 (1) the establishment of rules for conducting
12 the general business of the Agency, in a manner not
13 inconsistent with this Act;

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

15 (3) directing the establishment and mainte-
16 nance of divisions or other offices within the Agency,
17 in order to carry out the responsibilities of the Agen-
18 cy under this Act, and to satisfy the requirements of
19 other applicable law;

20 (4) to coordinate and oversee the operation of
21 all administrative, enforcement, and research activi-
22 ties of the Agency;

23 (5) to adopt and use a seal;

1 (6) to determine the character of and the neces-
2 sity for the obligations and expenditures of the
3 Agency;

4 (7) the appointment and supervision of per-
5 sonnel employed by the Agency;

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

9 (9) the use and expenditure of funds;

10 (10) implementing this Act through rules, or-
11 ders, guidance, interpretations, statements of policy,
12 investigations, and enforcement actions; and

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

15 (b) DELEGATION OF AUTHORITY.—The Director
16 may delegate to any duly authorized employee, representa-
17 tive, or agent any power vested in the Director or the
18 Agency by law, except that the Director may not delegate
19 the power to appoint the Deputy Director under section
20 301(b)(4)(A).

21 (c) AUTONOMY OF AGENCY REGARDING REC-
22 COMMENDATIONS AND TESTIMONY.—No officer or agency
23 of the United States shall have any authority to require
24 the Director or any other officer of the Agency to submit
25 legislative recommendations, or testimony or comments on

1 legislation, to any officer or agency of the United States
2 for approval, comments, or review prior to the submission
3 of such recommendations, testimony, or comments to the
4 Congress, if such recommendations, testimony, or com-
5 ments to the Congress include a statement indicating that
6 the views expressed therein are those of the Director or
7 such officer, and do not necessarily reflect the views of
8 the President.

9 **SEC. 303. RULEMAKING AUTHORITY.**

10 The Director may prescribe rules and issue orders
11 and guidance, as may be necessary or appropriate to en-
12 able the Agency to administer and carry out the purposes
13 and objectives of this Act, and to prevent evasions thereof.

14 **SEC. 304. PERSONNEL.**

15 (a) APPOINTMENT.—

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

20 (2) EMPLOYEES OF THE AGENCY.—The Direc-
21 tor is authorized to employ technologists, designers,
22 attorneys, investigators, economists, and other em-
23 ployees as the Director considers necessary to con-
24 duct the business of the Agency.

25 (b) AGENCY OMBUDSMAN.—

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

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

5 (A) act as a liaison between the Agency
6 and any affected person with respect to any
7 problem that such person may have in dealing
8 with the Agency, resulting from the regulatory
9 activities of the Agency; and

10 (B) assure that safeguards exist to encour-
11 age complainants to come forward and preserve
12 confidentiality.

13 **SEC. 305. COMPLAINTS OF INDIVIDUALS.**

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

24 (b) ROUTING COMPLAINTS TO STATES.—To the ex-
25 tent practicable, State agencies may receive appropriate

1 complaints from the systems established under subsection
2 (a), if—

3 (1) the State agency system has the functional
4 capacity to receive calls or electronic reports routed
5 by the Agency systems;

6 (2) the State agency has satisfied any condi-
7 tions of participation in the system that the Agency
8 may establish, including treatment of personal infor-
9 mation and sharing of information on complaint res-
10 olution or related compliance procedures and re-
11 sources; and

12 (3) participation by the State agency includes
13 measures necessary to provide for protection of per-
14 sonal information that conform to the standards for
15 protection of the confidentiality of personal informa-
16 tion and for data integrity and security that apply
17 to Federal agencies.

18 (c) DATA SHARING REQUIRED.—To facilitate inclu-
19 sion in the reports required by section 310 of the matters
20 regarding complaints of individuals required by subsection
21 (b)(4) of such section to be included in such reports, inves-
22 tigation and enforcement activities, and monitoring of the
23 privacy and security of personal information, the Agency
24 shall share information about complaints of individuals
25 with Federal and State agencies that have jurisdiction

1 over the privacy or security of personal information and
2 State attorneys general, subject to the standards applica-
3 ble to Federal agencies for protection of the confidentiality
4 of personal information and for data security and integ-
5 rity. Other Federal agencies that have jurisdiction over the
6 privacy or security of personal information shall share
7 data relating to complaints of individuals regarding the
8 privacy or security of personal information with the Agen-
9 cy, subject to the standards applicable to Federal agencies
10 for protection of confidentiality of personal information
11 and for data security and integrity.

12 **SEC. 306. USER ADVISORY BOARD.**

13 (a) ESTABLISHMENT REQUIRED.—The Director shall
14 establish a User Advisory Board to advise and consult
15 with the Agency in the exercise of its functions under this
16 Act, and to provide information on emerging practices re-
17 lating to the treatment of personal information by covered
18 entities, including regional trends, concerns, and other rel-
19 evant information.

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

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

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

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

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

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

15 (a) ESTABLISHMENT REQUIRED.—The Director shall
16 establish an Academic and Research Advisory Board to
17 advise and consult with the Agency in the exercise of its
18 functions under this Act, and to provide information on
19 emerging practices relating to the treatment of personal
20 information by covered entities, including regional trends,
21 concerns, and other relevant information.

22 (b) MEMBERSHIP.—In appointing the members of
23 the Academic and Research Advisory Board, the Director
24 shall seek to assemble individuals with academic and re-
25 search expertise in privacy, cybersecurity, computer

1 science, innovation, economics, law, and public policy,
2 without regard to party affiliation.

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

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

10 (1) be entitled to receive compensation at a rate
11 fixed by the Director while attending meetings of the
12 Academic and Research Advisory Board, including
13 travel time; and

14 (2) receive travel expenses, including per diem
15 in lieu of subsistence, in accordance with applicable
16 provisions under subchapter I of chapter 57 of title
17 5, United States Code.

18 **SEC. 308. SMALL BUSINESS AND INVESTOR ADVISORY**
19 **BOARD.**

20 (a) ESTABLISHMENT REQUIRED.—The Director shall
21 establish a Small Business and Investor Advisory Board
22 to advise and consult with the Agency in the exercise of
23 its functions under this Act, and to provide information
24 on emerging practices relating to the treatment of per-

1 sonal information by covered entities, including regional
2 trends, concerns, and other relevant information.

3 (b) MEMBERSHIP.—In appointing the members of
4 the Small Business and Investor Advisory Board, the Di-
5 rector shall seek to assemble representatives of small busi-
6 nesses and investors in small businesses, without regard
7 to party affiliation.

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

12 (d) COMPENSATION AND TRAVEL EXPENSES.—Mem-
13 bers of the Small Business and Investor Advisory Board
14 who are not full-time employees of the United States
15 shall—

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

20 (2) receive travel expenses, including per diem
21 in lieu of subsistence, in accordance with applicable
22 provisions under subchapter I of chapter 57 of title
23 5, United States Code.

1 **SEC. 309. CONSULTATION.**

2 The Director shall consult with Federal and State
3 agencies that have jurisdiction over the privacy or security
4 of personal information, State attorneys general, inter-
5 national and intergovernmental bodies that conduct activi-
6 ties relating to the privacy or security of personal informa-
7 tion, and agencies of other countries that are similar to
8 the Agency, as appropriate, to promote consistent regu-
9 latory treatment of the activities of covered entities relat-
10 ing to the privacy or security of personal information.

11 **SEC. 310. REPORTS.**

12 (a) **REPORTS REQUIRED.**—Not later than 6 months
13 after the date of the enactment of this Act, and every 6
14 months thereafter, the Director shall submit a report to
15 the President and to the Committee on Energy and Com-
16 merce, the Committee on the Judiciary, and the Com-
17 mittee on Appropriations of the House of Representatives
18 and the Committee on Commerce, Science, and Transpor-
19 tation, the Committee on the Judiciary, and the Com-
20 mittee on Appropriations of the Senate, and shall publish
21 such report on the website of the Agency.

22 (b) **CONTENTS.**—Each report required by subsection
23 (a) shall include—

24 (1) a discussion of the significant problems
25 faced by individuals with respect to the privacy or
26 security of personal information;

1 (2) a justification of the budget request of the
2 Agency for the preceding year, unless a justification
3 for such year was included in the preceding report
4 submitted under such subsection;

5 (3) a list of the significant rules and orders
6 adopted by the Agency, as well as other significant
7 initiatives conducted by the Agency, during the pre-
8 ceding 6-month period and the plan of the Agency
9 for rules, orders, or other initiatives to be under-
10 taken during the upcoming 6-month period;

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

16 (5) a list, with a brief statement of the issues,
17 of the public enforcement actions to which the Agen-
18 cy was a party during the preceding 6-month period;
19 and

20 (6) an assessment of significant actions by
21 State attorneys general or State agencies relating to
22 this Act or the rules prescribed under this Act dur-
23 ing the preceding 6-month period.

1 **SEC. 311. GRANTS FOR DEVELOPING OPEN-SOURCE MA-**
2 **CHINE LEARNING TRAINING DATA.**

3 The Director shall establish an Open-Source Machine
4 Learning Training Data Program and make grants
5 through the program to support the development of open-
6 source, voluntarily disclosed, personal information data
7 sets to be used for the training or development of machine
8 learning and artificial intelligence algorithms. The Direc-
9 tor shall promulgate regulations to implement the Pro-
10 gram and to consider any such data sets are in compliance
11 with this Act balancing any intrusion on the privacy of,
12 potential privacy harms to, and reasonable expectations of
13 individuals to whom the personal information relates.

14 **SEC. 312. ANNUAL AUDITS.**

15 The Director shall order an annual independent audit
16 of the operations and budget of the Agency.

17 **SEC. 313. INSPECTOR GENERAL.**

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

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

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

1 **SEC. 314. AUTHORIZATION OF APPROPRIATIONS.**

2 There are authorized to be appropriated to the Direc-
3 tor to carry out this Act \$550,000,000 for each of the
4 fiscal years 2020, 2021, 2022, 2023, and 2024.

5 **TITLE IV—ENFORCEMENT**

6 **SEC. 401. DEFINITIONS.**

7 In this title:

8 (1) **AGENCY INVESTIGATOR.**—The term “Agen-
9 cy investigator” means any attorney or investigator
10 employed by the Agency who is charged with the
11 duty of enforcing or carrying into effect any provi-
12 sion of this Act or a rule or order prescribed under
13 this Act.

14 (2) **ATTORNEY GENERAL.**—The term “attorney
15 general” means, with respect to a State, the attor-
16 ney general or chief law enforcement officer of the
17 State, or another official or agency designated by
18 the State to bring civil actions on behalf of the State
19 or the residents of the State.

20 (3) **CUSTODIAN.**—The term “custodian” means
21 the custodian or any deputy custodian designated by
22 the Agency.

23 (4) **DOCUMENTARY MATERIAL.**—The term
24 “documentary material” includes the original or any
25 copy of any book, document, record, report, memo-
26 randum, paper, communication, tabulation, chart,

1 logs, electronic files, or other data or data compila-
2 tions stored in any medium.

3 (5) VIOLATION.—The term “violation” means
4 any act or omission that, if proved, would constitute
5 a violation of any provision of this Act or a rule or
6 order prescribed under this Act.

7 (6) NON-PUBLIC INFORMATION.—The term
8 “non-public information” means information that
9 has not been disclosed in a criminal, civil, or admin-
10 istrative proceeding, in a government investigation,
11 report, or audit, or by the news media or other pub-
12 lic source of information, and that was not obtained
13 in violation of the law.

14 **SEC. 402. INVESTIGATIONS AND ADMINISTRATIVE DIS-**
15 **COVERY.**

16 (a) JOINT INVESTIGATIONS.—The Agency or, where
17 appropriate, an Agency investigator, may conduct inves-
18 tigation and make requests for information, as authorized
19 under this Act, on a joint basis with another agency (as
20 defined in section 551 of title 5, United States Code).

21 (b) SUBPOENAS.—

22 (1) IN GENERAL.—The Agency or an Agency
23 investigator may issue subpoenas for the attendance
24 and testimony of witnesses and the production of

1 relevant papers, books, documents, or other material
2 in connection with hearings under this Act.

3 (2) FAILURE TO OBEY.—In the case of contu-
4 macy or refusal to obey a subpoena issued pursuant
5 to this subsection and served upon any person, the
6 district court of the United States for any district in
7 which such person is found, resides, or transacts
8 business, upon application by the Agency or an
9 Agency investigator and after notice to such person,
10 may issue an order requiring such person to appear
11 and give testimony or to appear and produce docu-
12 ments or other material.

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

16 (c) DEMANDS.—

17 (1) IN GENERAL.—Whenever the Agency has
18 reason to believe that any person may be in posses-
19 sion, custody, or control of any documentary mate-
20 rial or tangible things, or may have any information,
21 relevant to a violation, the Agency may, before the
22 institution of any proceedings under this Act, issue
23 in writing, and cause to be served upon such person,
24 a civil investigative demand requiring such person
25 to—

1 (A) produce such documentary material for
2 inspection and copying or reproduction in the
3 form or medium requested by the Agency;

4 (B) submit such tangible things;

5 (C) file written reports or answers to ques-
6 tions;

7 (D) give oral testimony concerning docu-
8 mentary material, tangible things, or other in-
9 formation; or

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

12 (2) REQUIREMENTS.—Each civil investigative
13 demand shall state the nature of the conduct consti-
14 tuting the alleged violation which is under investiga-
15 tion and the provision of law applicable to such vio-
16 lation.

17 (3) PRODUCTION OF DOCUMENTS.—Each civil
18 investigative demand for the production of documen-
19 tary material shall—

20 (A) describe each class of documentary
21 material to be produced under the demand with
22 such definiteness and certainty as to permit
23 such material to be fairly identified;

24 (B) prescribe a return date or dates which
25 will provide a reasonable period of time within

1 which the material so demanded may be assem-
2 bled and made available for inspection and
3 copying or reproduction; and

4 (C) identify the custodian to whom such
5 material shall be made available.

6 (4) PRODUCTION OF THINGS.—Each civil inves-
7 tigative demand for the submission of tangible
8 things shall—

9 (A) describe each class of tangible things
10 to be submitted under the demand with such
11 definiteness and certainty as to permit such
12 things to be fairly identified;

13 (B) prescribe a return date or dates which
14 will provide a reasonable period of time within
15 which the things so demanded may be assem-
16 bled and submitted; and

17 (C) identify the custodian to whom such
18 things shall be submitted.

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

22 (A) propound with definiteness and cer-
23 tainty the reports to be produced or the ques-
24 tions to be answered;

1 (B) prescribe a date or dates at which time
2 written reports or answers to questions shall be
3 submitted; and

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

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

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

10 (B) identify an Agency investigator who
11 shall conduct the investigation and the custo-
12 dian to whom the transcript of such investiga-
13 tion shall be submitted.

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

17 (A) by any Agency investigator at any
18 place within the territorial jurisdiction of any
19 court of the United States; and

20 (B) upon any person who is not found
21 within the territorial jurisdiction of any court of
22 the United States—

23 (i) in such manner as the Federal
24 Rules of Civil Procedure prescribe for serv-
25 ice in a foreign nation; and

1 (ii) to the extent that the courts of
2 the United States have authority to assert
3 jurisdiction over such person, consistent
4 with due process, the United States Dis-
5 trict Court for the District of Columbia
6 shall have the same jurisdiction to take
7 any action respecting compliance with this
8 section by such person that such district
9 court would have if such person were per-
10 sonally within the jurisdiction of such dis-
11 trict court.

12 (8) METHOD OF SERVICE.—Service of any civil
13 investigative demand or any enforcement petition
14 filed under this section may be made upon a person
15 by—

16 (A) delivering a duly executed copy of such
17 demand or petition to the individual or to any
18 partner, executive officer, managing agent, or
19 general agent of such person, or to any agent
20 of such person authorized by appointment or by
21 law to receive service of process on behalf of
22 such person;

23 (B) delivering a duly executed copy of such
24 demand or petition to the principal office or
25 place of business of the person to be served; or

1 (C) depositing a duly executed copy in the
2 United States mails, by registered or certified
3 mail, return receipt requested, duly addressed
4 to such person at the principal office or place
5 of business of such person.

6 (9) PROOF OF SERVICE.—

7 (A) IN GENERAL.—A verified return by the
8 individual serving any civil investigative demand
9 or any enforcement petition filed under this sec-
10 tion setting forth the manner of such service
11 shall be proof of such service.

12 (B) RETURN RECEIPTS.—In the case of
13 service by registered or certified mail, such re-
14 turn shall be accompanied by the return post
15 office receipt of delivery of such demand or en-
16 forcement petition.

17 (10) PRODUCTION OF DOCUMENTARY MATE-
18 RIAL.—The production of documentary material in
19 response to a civil investigative demand shall be
20 made under a sworn certificate, in such form as the
21 demand designates, by the person, if a natural per-
22 son, to whom the demand is directed or, if not a
23 natural person, by any person having knowledge of
24 the facts and circumstances relating to such produc-
25 tion, to the effect that all of the documentary mate-

1 rial required by the demand and in the possession,
2 custody, or control of the person to whom the de-
3 mand is directed has been produced and made avail-
4 able to the custodian.

5 (11) SUBMISSION OF TANGIBLE THINGS.—The
6 submission of tangible things in response to a civil
7 investigative demand shall be made under a sworn
8 certificate, in such form as the demand designates,
9 by the person to whom the demand is directed or,
10 if not a natural person, by any person having knowl-
11 edge of the facts and circumstances relating to such
12 production, to the effect that all of the tangible
13 things required by the demand and in the posses-
14 sion, custody, or control of the person to whom the
15 demand is directed have been submitted to the cus-
16 todian.

17 (12) SEPARATE ANSWERS.—Each reporting re-
18 quirement or question in a civil investigative demand
19 shall be answered separately and fully in writing
20 under oath, unless it is objected to, in which event
21 the reasons for the objection shall be stated in lieu
22 of an answer, and it shall be submitted under a
23 sworn certificate, in such form as the demand des-
24 ignates, by the person, if a natural person, to whom
25 the demand is directed or, if not a natural person,

1 by any person responsible for answering each report-
2 ing requirement or question, to the effect that all in-
3 formation required by the demand and in the posses-
4 sion, custody, control, or knowledge of the person to
5 whom the demand is directed has been submitted.

6 (13) TESTIMONY.—

7 (A) IN GENERAL.—

8 (i) OATH AND RECORDATION.—The
9 examination of any person pursuant to a
10 demand for oral testimony served under
11 this subsection shall be taken before an of-
12 ficer authorized to administer oaths and
13 affirmations by the laws of the United
14 States or of the place at which the exam-
15 ination is held. The officer before whom
16 oral testimony is to be taken shall put the
17 witness on oath or affirmation and shall
18 personally, or by any individual acting
19 under the direction of and in the presence
20 of the officer, record the testimony of the
21 witness.

22 (ii) TRANSCRIPTION.—The testimony
23 shall be taken stenographically and tran-
24 scribed.

1 (B) PARTIES PRESENT.—Any Agency in-
2 vestigator before whom oral testimony is to be
3 taken shall exclude from the place where the
4 testimony is to be taken all other persons, ex-
5 cept the person giving the testimony, the attor-
6 ney for that person, the officer before whom the
7 testimony is to be taken, an investigator or rep-
8 resentative of an agency with which the Agency
9 is engaged in a joint investigation, and any ste-
10 nographer taking such testimony.

11 (C) LOCATION.—The oral testimony of any
12 person taken pursuant to a civil investigative
13 demand shall be taken in the judicial district of
14 the United States in which such person resides,
15 is found, or transacts business, or in such other
16 place as may be agreed upon by the Agency in-
17 vestigator before whom the oral testimony of
18 such person is to be taken and such person.

19 (D) ATTORNEY REPRESENTATION.—

20 (i) IN GENERAL.—Any person com-
21 pelled to appear under a civil investigative
22 demand for oral testimony pursuant to this
23 subsection may be accompanied, rep-
24 resented, and advised by an attorney.

1 (ii) AUTHORITY.—The attorney may
2 advise a person described in clause (i), in
3 confidence, either upon the request of such
4 person or upon the initiative of the attor-
5 ney, with respect to any question asked of
6 such person.

7 (iii) OBJECTIONS.—A person de-
8 scribed in clause (i), or the attorney for
9 that person, may object on the record to
10 any question, in whole or in part, and such
11 person shall briefly state for the record the
12 reason for the objection. An objection may
13 properly be made, received, and entered
14 upon the record when it is claimed that
15 such person is entitled to refuse to answer
16 the question on grounds of any constitu-
17 tional or other legal right or privilege, in-
18 cluding the privilege against self-incrimina-
19 tion, but such person shall not otherwise
20 object to or refuse to answer any question,
21 and such person or attorney shall not oth-
22 erwise interrupt the oral examination.

23 (iv) REFUSAL TO ANSWER.—If a per-
24 son described in clause (i) refuses to an-
25 swer any question—

1 (I) the Agency may petition the
2 district court of the United States
3 pursuant to this section for an order
4 compelling such person to answer
5 such question; and

6 (II) if the refusal is on grounds
7 of the privilege against self-incrimina-
8 tion, the testimony of such person
9 may be compelled in accordance with
10 the provisions of section 6004 of title
11 18, United States Code.

12 (E) TRANSCRIPTS.—For purposes of this
13 subsection—

14 (i) after the testimony of any witness
15 is fully transcribed, the Agency investi-
16 gator shall afford the witness (who may be
17 accompanied by an attorney) a reasonable
18 opportunity to examine the transcript;

19 (ii) the transcript shall be read to or
20 by the witness, unless such examination
21 and reading are waived by the witness;

22 (iii) any changes in form or substance
23 which the witness desires to make shall be
24 entered and identified upon the transcript
25 by the Agency investigator, with a state-

1 ment of the reasons given by the witness
2 for making such changes;

3 (iv) the transcript shall be signed by
4 the witness, unless the witness in writing
5 waives the signing, is ill, cannot be found,
6 or refuses to sign; and

7 (v) if the transcript is not signed by
8 the witness during the 30-day period fol-
9 lowing the date on which the witness is
10 first afforded a reasonable opportunity to
11 examine the transcript, the Agency investi-
12 gator shall sign the transcript and state on
13 the record the fact of the waiver, illness,
14 absence of the witness, or the refusal to
15 sign, together with any reasons given for
16 the failure to sign.

17 (F) CERTIFICATION BY INVESTIGATOR.—

18 The Agency investigator shall certify on the
19 transcript that the witness was duly sworn by
20 him or her and that the transcript is a true
21 record of the testimony given by the witness,
22 and the Agency investigator shall promptly de-
23 liver the transcript or send it by registered or
24 certified mail to the custodian.

1 (G) COPY OF TRANSCRIPT.—The Agency
2 investigator shall furnish a copy of the tran-
3 script (upon payment of reasonable charges for
4 the transcript) to the witness only, except that
5 the Agency may for good cause limit such wit-
6 ness to inspection of the official transcript of
7 his testimony.

8 (H) WITNESS FEES.—Any witness appear-
9 ing for the taking of oral testimony pursuant to
10 a civil investigative demand shall be entitled to
11 the same fees and mileage which are paid to
12 witnesses in the district courts of the United
13 States.

14 (d) CONFIDENTIAL TREATMENT OF DEMAND MATE-
15 RIAL.—

16 (1) IN GENERAL.—Documentary materials and
17 tangible things received as a result of a civil inves-
18 tigative demand shall be subject to requirements and
19 procedures regarding confidentiality, in accordance
20 with rules established by the Agency.

21 (2) DISCLOSURE TO CONGRESS.—No rule es-
22 tablished by the Agency regarding the confidentiality
23 of materials submitted to, or otherwise obtained by,
24 the Agency shall be intended to prevent disclosure to
25 either House of Congress or to an appropriate com-

1 mittee of the Congress, except that the Agency is
2 permitted to adopt rules allowing prior notice to any
3 party that owns or otherwise provided the material
4 to the Agency and had designated such material as
5 confidential.

6 (e) PETITION FOR ENFORCEMENT.—

7 (1) IN GENERAL.—Whenever any person fails
8 to comply with any civil investigative demand duly
9 served upon him under this section, or whenever sat-
10 isfactory copying or reproduction of material re-
11 quested pursuant to the demand cannot be accom-
12 plished and such person refuses to surrender such
13 material, the Agency, through such officers or attor-
14 neys as it may designate, may file, in the district
15 court of the United States for any judicial district
16 in which such person resides, is found, or transacts
17 business, and serve upon such person, a petition for
18 an order of such court for the enforcement of this
19 section.

20 (2) SERVICE OF PROCESS.—All process of any
21 court to which application may be made as provided
22 in this subsection may be served in any judicial dis-
23 trict.

24 (f) PETITION FOR ORDER MODIFYING OR SETTING
25 ASIDE DEMAND.—

1 (1) IN GENERAL.—Not later than 20 days after
2 the service of any civil investigative demand upon
3 any person under subsection (c), or at any time be-
4 fore the return date specified in the demand, which-
5 ever period is shorter, or within such period exceed-
6 ing 20 days after service or in excess of such return
7 date as may be prescribed in writing, subsequent to
8 service, by any Agency investigator named in the de-
9 mand, such person may file with the Agency a peti-
10 tion for an order by the Agency modifying or setting
11 aside the demand.

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

19 (3) SPECIFIC GROUNDS.—A petition under
20 paragraph (1) shall specify each ground upon which
21 the petitioner relies in seeking relief, and may be
22 based upon any failure of the demand to comply
23 with the provisions of this section, or upon any con-
24 stitutional or other legal right or privilege of such
25 person.

1 (g) CUSTODIAL CONTROL.—At any time during
2 which any custodian is in custody or control of any docu-
3 mentary material, tangible things, reports, answers to
4 questions, or transcripts of oral testimony given by any
5 person in compliance with any civil investigative demand,
6 such person may file, in the district court of the United
7 States for the judicial district within which the office of
8 such custodian is situated, and serve upon such custodian,
9 a petition for an order of such court requiring the per-
10 formance by such custodian of any duty imposed upon him
11 by this section or rule promulgated by the Agency.

12 (h) JURISDICTION OF COURT.—

13 (1) IN GENERAL.—Whenever any petition is
14 filed in any district court of the United States under
15 this section, such court shall have jurisdiction to
16 hear and determine the matter so presented, and to
17 enter such order or orders as may be required to
18 carry out the provisions of this section.

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

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

24 (a) IN GENERAL.—The Agency is authorized to con-
25 duct hearings and adjudication proceedings with respect

1 to any person in the manner prescribed by chapter 5 of
2 title 5, United States Code, in order to ensure or enforce
3 compliance with this Act and the rules prescribed under
4 this Act.

5 (b) SPECIAL RULES FOR CEASE-AND-DESIST PRO-
6 CEEDINGS.—

7 (1) ORDERS AUTHORIZED.—

8 (A) IN GENERAL.—If, in the opinion of the
9 Agency, a person is engaging or has engaged in
10 an act or omission that violates any provision of
11 this Act or a rule or order prescribed under this
12 Act, the Agency may issue and serve upon the
13 person a notice of charges in respect thereof.

14 (B) CONTENT OF NOTICE.—The notice
15 under subparagraph (A) shall contain a state-
16 ment of the facts constituting the alleged viola-
17 tion, and shall fix a time and place at which a
18 hearing will be held to determine whether an
19 order to cease and desist should issue against
20 the person, such hearing to be held not earlier
21 than 30 days nor later than 60 days after the
22 date of service of such notice, unless an earlier
23 or a later date is set by the Agency, at the re-
24 quest of any person so served.

1 (C) CONSENT.—Unless a person served
2 under subparagraph (B) appears at the hearing
3 personally or by a duly authorized representa-
4 tive, the person shall be deemed to have con-
5 sented to the issuance of the cease-and-desist
6 order.

7 (D) PROCEDURE.—In the event of consent
8 under subparagraph (C), or if, upon the record
9 made at any such hearing, the Agency finds
10 that any violation specified in the notice of
11 charges has been established, the Agency may
12 issue and serve upon the person an order to
13 cease and desist from the violation. Such order
14 may, by provisions which may be mandatory or
15 otherwise, require the person to cease and de-
16 sist from the subject act or omission, and to
17 take affirmative action to correct the conditions
18 resulting from any such violation.

19 (2) EFFECTIVENESS OF ORDER.—A cease-and-
20 desist order shall become effective at the expiration
21 of 30 days after the date of service of the order
22 under paragraph (1)(D) (except in the case of a
23 cease-and-desist order issued upon consent, which
24 shall become effective at the time specified therein),
25 and shall remain effective and enforceable as pro-

1 vided therein, except to such extent as the order is
2 stayed, modified, terminated, or set aside by action
3 of the Agency or a reviewing court.

4 (3) DECISION AND APPEAL.—Any hearing pro-
5 vided for in this subsection shall be held in the Fed-
6 eral judicial district or in the territory in which the
7 residence or principal office or place of business of
8 the person is located unless the person consents to
9 another place, and shall be conducted in accordance
10 with the provisions of chapter 5 of title 5, United
11 States Code. After such hearing, and not later than
12 90 days after the Agency has notified each party to
13 the proceeding that the case has been submitted to
14 the Agency for final decision, the Agency shall
15 render its decision (which shall include findings of
16 fact upon which its decision is predicated) and shall
17 issue and serve upon each such party an order or or-
18 ders consistent with the provisions of this section.
19 Judicial review of any such order shall be exclusively
20 as provided in this subsection. Unless a petition for
21 review is timely filed in a court of appeals of the
22 United States, as provided in paragraph (4), and
23 thereafter until the record in the proceeding has
24 been filed as provided in paragraph (4), the Agency
25 may at any time, upon such notice and in such man-

1 ner as the Agency shall determine proper, modify,
2 terminate, or set aside any such order. Upon filing
3 of the record as provided, the Agency may modify,
4 terminate, or set aside any such order with permis-
5 sion of the court.

6 (4) APPEAL TO COURT OF APPEALS.—Any
7 party to any proceeding under this subsection may
8 obtain a review of any order served pursuant to this
9 subsection (other than an order issued with the con-
10 sent of the party) by filing in the court of appeals
11 of the United States for the circuit in which the resi-
12 dence or principal office or place of business of the
13 party is located, or in the United States Court of
14 Appeals for the District of Columbia Circuit, within
15 30 days after the date of service of such order, a
16 written petition praying that the order of the Agency
17 be modified, terminated, or set aside. A copy of such
18 petition shall be forthwith transmitted by the clerk
19 of the court to the Agency, and thereupon the Agen-
20 cy shall file in the court the record in the pro-
21 ceeding, as provided in section 2112 of title 28,
22 United States Code. Upon the filing of such petition,
23 such court shall have jurisdiction, which upon the
24 filing of the record shall, except as provided in the
25 last sentence of paragraph (3), be exclusive, to af-

1 firm, modify, terminate, or set aside, in whole or in
2 part, the order of the Agency. Review of such pro-
3 ceedings shall be had as provided in chapter 7 of
4 title 5, United States Code. The judgment and de-
5 cree of the court shall be final, except that the same
6 shall be subject to review by the Supreme Court of
7 the United States, upon certiorari, as provided in
8 section 1254 of title 28, United States Code.

9 (5) NO STAY.—The commencement of pro-
10 ceedings for judicial review under paragraph (4)
11 shall not, unless specifically ordered by the court,
12 operate as a stay of any order issued by the Agency.

13 (c) SPECIAL RULES FOR TEMPORARY CEASE-AND-
14 DESIST PROCEEDINGS.—

15 (1) IN GENERAL.—Whenever the Agency deter-
16 mines that the violation specified in the notice of
17 charges served upon a person pursuant to subsection
18 (b), or the continuation thereof, is likely to cause the
19 person to be insolvent or otherwise prejudice the in-
20 terests of individuals before the completion of the
21 proceedings conducted pursuant to subsection (b),
22 the Agency may issue a temporary order requiring
23 the person to cease and desist from any such viola-
24 tion and to take affirmative action to prevent or
25 remedy such insolvency or other condition pending

1 completion of such proceedings. Such order may in-
2 clude any requirement authorized under this title.
3 Such order shall become effective upon service upon
4 the person and, unless set aside, limited, or sus-
5 pended by a court in proceedings authorized by
6 paragraph (2), shall remain effective and enforceable
7 pending the completion of the administrative pro-
8 ceedings pursuant to such notice and until such time
9 as the Agency shall dismiss the charges specified in
10 such notice, or if a cease-and-desist order is issued
11 against the person, until the effective date of such
12 order.

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

1 (d) SPECIAL RULES FOR ENFORCEMENT OF OR-
2 DERS.—

3 (1) IN GENERAL.—The Agency may in its dis-
4 cretion apply to the United States district court
5 within the jurisdiction of which the residence or
6 principal office or place of business of a person is lo-
7 cated, for the enforcement of any effective and out-
8 standing order issued under this section against
9 such person, and such court shall have jurisdiction
10 and power to order and require compliance with
11 such order.

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

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

20 **SEC. 404. LITIGATION AUTHORITY.**

21 (a) IN GENERAL.—If a person violates any provision
22 of this Act or a rule or order prescribed under this Act,
23 the Agency may commence a civil action against such per-
24 son to impose a civil penalty or to seek all appropriate

1 legal and equitable relief, including a permanent or tem-
2 porary injunction.

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

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

11 (d) NOTICE TO THE ATTORNEY GENERAL.—

12 (1) IN GENERAL.—When commencing a civil
13 action under subsection (a), the Agency shall notify
14 the Attorney General.

15 (2) NOTICE AND COORDINATION.—

16 (A) NOTICE OF OTHER ACTIONS.—In addi-
17 tion to any notice required under paragraph
18 (1), the Agency shall notify the Attorney Gen-
19 eral concerning any action, suit, or other court
20 proceeding to which the Agency is a party.

21 (B) COORDINATION.—In order to avoid
22 conflicts and promote consistency regarding liti-
23 gation of matters under Federal law, the Attor-
24 ney General and the Agency shall consult re-
25 garding the coordination of investigations and

1 proceedings, including by negotiating an agree-
2 ment for coordination by not later than 180
3 days after the effective date specified in section
4 4(a). The agreement under this subparagraph
5 shall include provisions to ensure that parallel
6 investigations and proceedings involving this
7 Act and the rules prescribed under this Act are
8 conducted in a manner that avoids conflicts and
9 does not impede the ability of the Attorney
10 General to prosecute violations of Federal
11 criminal laws.

12 (C) RULE OF CONSTRUCTION.—Nothing in
13 this paragraph shall be construed to limit the
14 authority of the Agency under this Act, includ-
15 ing the authority to interpret this Act.

16 (e) APPEARANCE BEFORE THE SUPREME COURT.—
17 The Agency may represent itself in its own name before
18 the Supreme Court of the United States, if the Agency
19 makes a written request to the Attorney General within
20 the 10-day period which begins on the date of entry of
21 the judgment which would permit any party to file a peti-
22 tion for writ of certiorari, and the Attorney General con-
23 curs with such request or fails to take action within 60
24 days of the request of the Agency.

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

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

8 **SEC. 405. COORDINATION WITH OTHER FEDERAL AGEN-**
9 **CIES.**

10 (a) COORDINATION.—With respect to covered entities
11 and service providers, to the extent that Federal law au-
12 thorizes the Agency and another Federal agency to enforce
13 privacy laws, the other Federal agency shall coordinate
14 with the Agency to promote consistent enforcement of this
15 Act and other Federal privacy laws.

16 (b) REFERRAL.—Any Federal agency authorized to
17 enforce a Federal privacy law described in section 501
18 may recommend in writing to the Agency that the Agency
19 initiate an enforcement proceeding, as the Agency is au-
20 thorized by that Federal law or by this Act.

21 (c) COORDINATION WITH THE FEDERAL TRADE
22 COMMISSION.—

23 (1) IN GENERAL.—The Agency and the Federal
24 Trade Commission shall negotiate an agreement for
25 coordinating with respect to enforcement actions by

1 each agency regarding the provision of a product or
2 service offered by any covered entity. The agreement
3 shall include procedures for notice to the other agen-
4 cy, where feasible, prior to initiating a civil action to
5 enforce any Federal law regarding the privacy of in-
6 dividuals or security of personal information.

7 (2) CIVIL ACTIONS.—Whenever a civil action
8 has been filed by, or on behalf of, the Agency or the
9 Federal Trade Commission for any violation of any
10 provision of Federal law described in paragraph (1),
11 or any regulation prescribed under such provision of
12 law—

13 (A) the other agency may not, during the
14 pendency of that action, institute a civil action
15 under such provision of law against any defend-
16 ant named in the complaint in such pending ac-
17 tion for any violation alleged in the complaint;
18 and

19 (B) the Agency or the Federal Trade Com-
20 mission may intervene as a party in any such
21 action brought by the other agency, and, upon
22 intervening—

23 (i) be heard on all matters arising in
24 such enforcement action; and

1 (ii) file petitions for appeal in such ac-
2 tions.

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

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

9 **SEC. 406. ENFORCEMENT BY STATES.**

10 (a) CIVIL ACTION.—In any case in which the attor-
11 ney general of a State has reason to believe that an inter-
12 est of the residents of such State has been or is adversely
13 affected by any person who violates any provision of this
14 Act or a rule or order prescribed under this Act, the attor-
15 ney general of the State, as *parens patriae*, may bring a
16 civil action on behalf of the residents of the State in an
17 appropriate State court or an appropriate district court
18 of the United States—

19 (1) to enjoin further violation of such provision
20 by the defendant;

21 (2) to compel compliance with such provision;

22 or

23 (3) to obtain relief under section 408.

24 (b) RIGHTS OF AGENCY.—Before initiating a civil ac-
25 tion under subsection (a), the attorney general of a State

1 shall notify the Agency in writing of such civil action.

2 Upon receiving notice with respect to a civil action, the

3 Agency may—

4 (1) intervene in such action; and

5 (2) upon intervening—

6 (A) be heard on all matters arising in such

7 civil action; and

8 (B) file petitions for appeal of a decision in

9 such action.

10 (c) **PREEMPTIVE ACTION BY AGENCY.**—If the Agen-

11 cy institutes a civil action for violation of any provision

12 of this Act or a rule or order prescribed under this Act,

13 no attorney general of a State may bring a civil action

14 against any defendant named in the complaint of the

15 Agency for a violation of such provision that is alleged

16 in such complaint.

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

18 (a) **INJUNCTIVE RELIEF.**—A person who is aggrieved

19 by a violation of this Act may bring a civil action for de-

20 claratory or injunctive relief in any court of competent ju-

21 risdiction in any State or in an appropriate district court.

22 (b) **CIVIL ACTION FOR DAMAGES.**—Except for claims

23 under rule 23 of the Federal Rules of Civil Procedure or

24 a similar judicial procedure authorizing an action to be

25 brought by 1 or more representatives, a person who is ag-

1 grieved by a violation of this Act may bring a civil action
2 for damages in any court of competent jurisdiction in any
3 State or in an appropriate district court.

4 (c) NONPROFIT COLLECTIVE REPRESENTATION.—

5 An individual shall have the right to appoint a nonprofit
6 body, organization, or association which has been properly
7 constituted in accordance with the law, has statutory ob-
8 jectives which are in the public interest, and is active in
9 the field of the protection of individual rights and free-
10 doms with regard to the protection of their personal data
11 to lodge the complaint on his or her behalf, to exercise
12 the rights referred to in this Act on his or her behalf.

13 (1) A nonprofit may represent a class of ag-
14 grieved individuals.

15 (2) A prevailing nonprofit shall receive reason-
16 able compensation for expenses, including attorneys
17 fees.

18 (3) Individuals shall receive an equally divided
19 share of the total damages.

20 (d) STATE APPOINTMENT.—A State may provide
21 that any body, organization or association referred to in
22 subsection (c), independently of an individual's appoint-
23 ment, has the right to lodge, in that State, a complaint
24 with the Agency and to exercise the rights referred to in

1 this Act if it considers that the rights of an individual
2 under this Act have been infringed.

3 **SEC. 408. RELIEF AVAILABLE.**

4 (a) CIVIL ACTIONS AND ADJUDICATION PRO-
5 CEEDINGS.—

6 (1) JURISDICTION.—In any civil action or any
7 adjudication proceeding brought by the Agency or
8 the attorney general of a State, under any provision
9 of this Act or a rule or order prescribed under this
10 Act, the court or the Agency (as the case may be)
11 shall have jurisdiction to grant any appropriate legal
12 or equitable relief with respect to a violation of such
13 provision.

14 (2) RELIEF.—Relief under this section may in-
15 clude—

16 (A) rescission or reformation of contracts;

17 (B) refund of moneys;

18 (C) restitution;

19 (D) disgorgement or compensation for un-
20 just enrichment;

21 (E) payment of damages or other mone-
22 tary relief;

23 (F) public notification regarding the viola-
24 tion, including the costs of notification;

1 (G) limits on the activities or functions of
2 the person; and

3 (H) civil money penalties, as provided in
4 subsection (c).

5 (3) NO EXEMPLARY OR PUNITIVE DAMAGES.—
6 Nothing in this subsection shall be construed as au-
7 thorizing the imposition of exemplary or punitive
8 damages.

9 (b) RECOVERY OF COSTS.—In any civil action
10 brought by the Agency or the attorney general of a State
11 under any provision of this Act or a rule or order pre-
12 scribed under this Act, the Agency or attorney general
13 may recover its costs in connection with prosecuting such
14 action if the Agency or attorney general is the prevailing
15 party in the action.

16 (c) CIVIL MONEY PENALTY IN COURT AND ADJU-
17 DICATION PROCEEDINGS.—

18 (1) IN GENERAL.—Any person who violates,
19 through any act or omission, any provision of this
20 Act or a rule or order prescribed under this Act
21 shall forfeit and pay a civil penalty under this sub-
22 section.

23 (2) PENALTY AMOUNT.—

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

4 (i) the maximum civil penalty for
5 which a person, partnership, or corporation
6 may be liable under section 5(m)(1)(A) of
7 the Federal Trade Commission Act (15
8 U.S.C. 45(m)(1)(A)) for a violation of a
9 rule under such Act respecting unfair or
10 deceptive acts or practices, as adjusted
11 under the Federal Civil Penalties Inflation
12 Adjustment Act of 1990 (28 U.S.C. 2461
13 note); and

14 (ii) the number of individuals the per-
15 sonal information of which is affected by
16 the violation.

17 (B) CONTINUING VIOLATIONS.—In the
18 case of a violation through continuing failure to
19 comply with a provision of this Act or a rule or
20 order prescribed under this Act, each day of
21 continuance of such failure shall be treated as
22 a separate violation for purposes of subpara-
23 graph (A).

24 (3) MITIGATING FACTORS.—In determining the
25 amount of any penalty assessed under paragraph

1 (2), the court or the Agency shall take into account
2 the appropriateness of the penalty with respect to—

3 (A) the size of financial resources and good
4 faith of the person charged;

5 (B) the gravity of the violation;

6 (C) the severity of the privacy harms (in-
7 cluding both actual and potential harms) to in-
8 dividuals;

9 (D) any disparate impact of the privacy
10 harms (including both actual and potential
11 harms) on protected classes;

12 (E) the history of previous violations; and

13 (F) such other matters as justice may re-
14 quire.

15 (4) AUTHORITY TO MODIFY OR REMIT PEN-
16 ALTY.—The Agency or attorney general of a State
17 may compromise, modify, or remit any penalty which
18 may be assessed or has already been assessed under
19 paragraph (2). The amount of such penalty, when fi-
20 nally determined, shall be exclusive of any sums
21 owed by the person to the United States in connec-
22 tion with the costs of the proceeding, and may be
23 deducted from any sums owing by the United States
24 to the person charged.

1 (5) NOTICE AND HEARING.—No civil penalty
2 may be assessed under this subsection with respect
3 to a violation of any provision of this Act or a rule
4 or order prescribed under this Act, unless—

5 (A) the Agency or attorney general of a
6 State gives notice and an opportunity for a
7 hearing to the person accused of the violation;
8 or

9 (B) the appropriate court has ordered such
10 assessment and entered judgment in favor of
11 the Agency or attorney general of a State.

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

13 If the Agency obtains evidence that any person, do-
14 mestic or foreign, has engaged in conduct that may con-
15 stitute a violation of Federal criminal law, the Agency
16 shall transmit such evidence to the Attorney General of
17 the United States, who may institute criminal proceedings
18 under appropriate law. Nothing in this section affects any
19 other authority of the Agency to disclose information.

20 **SEC. 410. WHISTLEBLOWER ENFORCEMENT.**

21 (a) IN GENERAL.—Any person who becomes aware,
22 based on non-public information, that a covered entity has
23 violated this Act may file a civil action for civil penalties,
24 if prior to filing such action, the person files with the Di-
25 rector a written request for the Director to commence the

1 action. The request shall include a clear and concise state-
2 ment of the grounds for believing a cause of action exists.
3 The person shall make the non-public information avail-
4 able to the Director upon request:

5 (1) If the Director files suit within 90 days
6 from receipt of the written request to commence the
7 action, no other action may be brought unless the
8 action brought by the Director is dismissed without
9 prejudice.

10 (2) If the Director does not file suit within 90
11 days from receipt of the written request to com-
12 mence the action, the person requesting the action
13 may proceed to file a civil action.

14 (3) The time period within which a civil action
15 shall be commenced shall be tolled from the date of
16 receipt by the Director of the written request to ei-
17 ther the date that the civil action is dismissed with-
18 out prejudice, or for 150 days, whichever is later,
19 but only for a civil action brought by the person who
20 requested the Director to commence the action.

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

1 (D) the Fair Debt Collection Practices Act
2 (15 U.S.C. 1692 et seq.);

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

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

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

9 (H) section 444 of the General Education
10 Provisions Act (20 U.S.C. 1232g) (commonly
11 referred to as the “Family Educational Rights
12 and Privacy Act of 1974”);

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

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

17 (K) the regulations promulgated under sec-
18 tion 264(e) of the Health Insurance Portability
19 and Accountability Act of 1996 (42 U.S.C.
20 1320d–2 note), as those regulations relate to—

21 (i) a person described in section
22 1172(a) of the Social Security Act (42
23 U.S.C. 1320d–1(a)); or

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

4 (L) the Communications Assist-
5 ance for Law Enforcement Act (47
6 U.S.C. 1001 et seq.);

7 (M) section 222, 227, 338, or 631 of the
8 Communications Act of 1934 (47 U.S.C. 222,
9 227, 338, or 551);

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

12 (O) the Paperwork Reduction Act of 1995
13 (44 U.S.C. 3501 et seq.);

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

16 (Q) the Currency and Foreign Trans-
17 actions Reporting Act of 1970, as amended
18 (commonly known as the Bank Secrecy Act)
19 (12 U.S.C. 1829b and 1951–1959, 31 U.S.C.
20 5311–5314 and 5316–5332), including the
21 International Money Laundering Abatement
22 and Financial Anti-Terrorism Act of 2001, title
23 III of Public Law 107–56, as amended;

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

1 (S) the Foreign Intelligence Surveillance
2 Act of 1978, as amended (50 U.S.C. 1801 et
3 seq.);

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

6 (U) the Americans with Disabilities Act
7 (42 U.S.C. 12101 et seq.);

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

10 (W) the Dodd-Frank Wall Street Reform
11 and Consumer Protection Act (Public Law
12 111–203, 124 Stat. 1376–2223);

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

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

17 (Z) the Genetic Information Non-
18 discrimination Act (Public Law 110–233, 122
19 Stat. 881); or

20 (AA) any other privacy or security provi-
21 sion of Federal law; or

22 (2) limit the authority of the Federal Commu-
23 nications Commission to promulgate regulations and
24 enforce any privacy law not in contradiction with
25 this Act.

1 **SEC. 502. SEVERABILITY.**

2 If any provision of this Act, or the application there-
3 of, is held unconstitutional or otherwise invalid, the valid-
4 ity of the remainder of the Act and the application of such
5 provision shall not be affected thereby.

○