

119TH CONGRESS
2D SESSION

H. R. 8014

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 Digital Privacy Agency to enforce such rights and requirements, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 19, 2026

Ms. LOFGREN introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committees on the Judiciary, and Science, Space, and Technology, 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 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 2026”.

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. General provisions.
- Sec. 4. Limitation on disclosing nonredacted government records.
- Sec. 5. Criminal prohibition on doxxing.

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.
- Sec. 202. Minimization and records of access by employees and contractors.
- Sec. 203. Prohibitions on disclosing of personal information.
- Sec. 204. Disclosing to entities not subject to United States jurisdiction or not compliant with this Act.
- Sec. 205. Prohibition on re-identification.
- Sec. 206. Restrictions on collecting, processing, maintaining, and disclosing contents of communications.
- Sec. 207. Prohibition on discriminatory processing.
- Sec. 208. Requirements for notice and consent processes and privacy policies.
- Sec. 209. Prohibition on “dark patterns” in notice and consent processes and privacy policies.
- Sec. 210. Notice and consent required.
- Sec. 211. Privacy policy.
- Sec. 212. Information security requirements.
- Sec. 213. Notification of data breach or data-sharing abuse.

TITLE III—DIGITAL PRIVACY AGENCY

- Sec. 301. Establishment; Director and Deputy Director.
- Sec. 302. Agency powers and authorities.
- Sec. 303. Reporting and audit requirements.
- Sec. 304. Relation to other agencies.
- Sec. 305. Personnel.

- Sec. 306. Office of Civil Rights.
- Sec. 307. Complaints of individuals.
- Sec. 308. Advisory boards.
- Sec. 309. Authorization of appropriations.

TITLE IV—ENFORCEMENT

- Sec. 401. Investigations and administrative discovery.
- Sec. 402. Hearings and adjudication proceedings.
- Sec. 403. Litigation authority.
- Sec. 404. Enforcement by States.
- Sec. 405. Private rights of action.
- Sec. 406. Relief available.
- Sec. 407. Referral for criminal proceedings.
- Sec. 408. Whistleblower enforcement.

TITLE V—RELATION TO OTHER LAW

- Sec. 501. Effective date.
- Sec. 502. Relation to other Federal law.
- Sec. 503. Relation to State law.
- Sec. 504. Severability.

TITLE VI—NIST AND NSF ACTIVITIES

- Sec. 601. National Institute of Standards and Technology privacy research and development.
- Sec. 602. National privacy awareness and education initiative.
- Sec. 603. National Science Foundation privacy research.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) BEHAVIORAL PERSONALIZATION.—

4 (A) IN GENERAL.—The term “behavioral
5 personalization” means the processing of the
6 personal information of an individual, using an
7 algorithm, model, or other means—

8 (i) built using—

9 (I) that individual’s personal in-
10 formation collected over a period of
11 time; or

1 (II) an aggregate of the informa-
2 tion of one or more similarly situated
3 individuals; and

4 (ii) designed to—

5 (I) alter, influence, guide, or pre-
6 dict that individual’s behavior;

7 (II) tailor or personalize a prod-
8 uct or service to that individual; or

9 (III) filter, sort, limit, promote,
10 display or otherwise differentiate be-
11 tween specific content or categories of
12 content that would otherwise be acces-
13 sible to that individual.

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

19 (2) COLLECT.—The term “collect” includes,
20 with respect to personal information or the contents
21 of any communication, obtaining such information or
22 contents in any manner, except when solely trans-
23 mitting, routing, providing intermediate storage for,
24 or providing connections for such personal informa-
25 tion or communication through a system or network.

1 (3) COMMISSION.—The term “Commission”
2 means the Federal Trade Commission.

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

7 (5) COVERED ENTITY.—

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

10 (i) intentionally collects, processes, or
11 maintains personal information; and

12 (ii) sends or receives such personal in-
13 formation over the internet or a similar
14 communications network.

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

19 (C) DE MINIMIS DEFINED.—In this para-
20 graph, the term “de minimis” means incidental
21 commercial activity by a natural person that—

22 (i) generates not more than \$5,000 in
23 gross revenue in a 12-month period; or

1 (ii) involves the personal information
2 of fewer than 5,000 individuals in such pe-
3 riod.

4 (6) CUSTODIAN.—The term “custodian” means
5 the custodian or any deputy custodian designated by
6 the Director of the Digital Privacy Agency.

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

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

16 (A) a purpose specified by the covered en-
17 tity to the third party at the time such personal
18 information or contents of communications was
19 disclosed; or

20 (B) a purpose to which the individual to
21 whom the information relates has consented.

22 (9) DE-IDENTIFY.—

23 (A) IN GENERAL.—The term “de-identify”
24 means, with respect to information, performing
25 actions so that such information cannot reason-

ably identify, relate to, describe, reference, be
capable of being associated with, or be linked,
directly or indirectly, to a particular individual
or device, but only to the extent that the covered
entity that uses such information—

(i) has performed such actions using
best practices for the types of data such
information contains;

(ii) has implemented technical safeguards that prohibit re-identification of the
individual with whom such information was
linked;

(iii) has implemented business processes that specifically prohibit re-identification of the information;

(iv) has implemented business processes to prevent inadvertent release of such
information; and

(v) makes no attempt to re-identify
such information.

(B) DETERMINATION BY THE DIRECTOR.—

The Director may determine that a methodology of de-identifying personal information is
insufficient for the purposes of this paragraph.

1 (10) DIGITAL PRIVACY AGENCY.—The term
2 “Digital Privacy Agency” means the Digital Privacy
3 Agency established under section 301.

4 (11) DIGITAL PRIVACY AGENCY INVESTI-
5 GATOR.—The term “Digital Privacy agency investi-
6 gator” means any attorney or investigator employed
7 by the Digital Privacy Agency who is charged with
8 the enforcement of or carrying out of any provision
9 of this Act or a rule or order prescribed under this
10 Act.

11 (12) DIRECTOR.—The term “Director” means
12 the Director of the Digital Privacy Agency.

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

19 (14) DOCUMENTARY MATERIAL.—The term
20 “documentary material” includes the original or any
21 copy of any book, document, record, report, memo-
22 randum, paper, communication, tabulation, chart,
23 logs, electronic files, or other data or data compila-
24 tions stored in any medium.

1 (15) FEDERAL AGENCY.—The term “Federal
2 agency” has the meaning given that term in section
3 3371 of title 5, United States Code.

4 (16) FEDERAL PRIVACY LAWS.—The term
5 “Federal privacy laws” includes the laws and regula-
6 tions described in section 502.

7 (17) GOVERNMENT ENTITY.—The term “gov-
8 ernment entity” means—

9 (A) a Federal agency;

10 (B) a State or political subdivision thereof;

11 or

12 (C) any agency, authority, or instrumen-
13 tality of a State or political subdivision thereof.

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

17 (19) INDIAN TRIBE.—The term “Indian Tribe”
18 has the meaning given such term in section 4(e) of
19 the Indian Self-Determination and Education Assist-
20 ance Act (25 U.S.C. 5304(e)).

21 (20) MAINTAIN.—The term “maintain” means,
22 with respect to personal information or the contents
23 of any communication, to store, secure, or otherwise
24 cause the retention of such information or contents,
25 or to take actions necessary for storing, securing, or

1 otherwise causing the retention of such information
2 or contents.

3 (21) NONPUBLIC INFORMATION.—The term
4 “nonpublic information” means information that has
5 not been disclosed in a criminal, civil, or administra-
6 tive proceeding, in a government investigation, re-
7 port, or audit, or by the news media or other public
8 source of information, and that was not obtained in
9 violation of the law.

10 (22) PERSONAL INFORMATION.—

11 (A) IN GENERAL.—The term “personal in-
12 formation” means any information maintained
13 by a covered entity that, on its own or com-
14 bined with other information, is linked or rea-
15 sonably linkable to a specific individual or a
16 specific device, including de-identified personal
17 information and the means to behavioral per-
18 sonalization created for or linked to a specific
19 individual.

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

22 (i) publicly available information
23 linked to an individual if that information
24 was not unlawfully made public; or

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

5 (23) PRIVACY HARM.—The term “privacy
6 harm” means an adverse consequence or a potential
7 adverse consequence to an individual, a group of in-
8 dividuals, or society caused from collecting, proc-
9 essing, maintaining, or disclosing of personal infor-
10 mation or contents of communications, including—

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

13 (B) physical harm;

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

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

25 (E) stigmatization or reputational harm;

1 (F) price discrimination;

2 (G) adverse consequences that affect the
3 private life of an individual, including private
4 family matters and actions and communications
5 within the home of such individual or a similar
6 physical, online, or digital location where such
7 individual has a reasonable expectation that
8 personal information will not be collected, proc-
9 essed, or maintained;

10 (H) the chilling of free expression or action
11 of an individual, a group of individuals, or soci-
12 ety, due to perceived or actual pervasive and ex-
13 cessive collecting, processing, disclosing, or
14 maintaining of personal information or contents
15 of communications;

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

18 (J) other adverse consequences or potential
19 adverse consequences, consistent with the provi-
20 sions of this Act, as determined by the Direc-
21 tor.

22 (24) PRIVACY-PRESERVING COMPUTING.—

23 (A) IN GENERAL.—The term “privacy-pre-
24 serving computing” means the collecting, proc-
25 essing, disclosing, or maintaining of personal

1 information that has been encrypted or other-
2 wise rendered unintelligible using a means that
3 cannot be reversed by a covered entity, or a
4 covered entity's service provider, such that—

5 (i) if such personal information could
6 be rendered intelligible through cooperation
7 or sharing of cryptographic secrets by mul-
8 tiple persons, the covered entity has both
9 technical safeguards and business proc-
10 esses to prevent such cooperation or shar-
11 ing;

12 (ii) if such personal information is
13 rendered intelligible within a hardware
14 processing unit or other means of per-
15 forming operations on the information,
16 there are technical safeguards that, during
17 the normal course of operation—

18 (I) prevent rendering personal in-
19 formation intelligible anywhere but
20 within the hardware processing unit
21 or other means of performing oper-
22 ations; and

23 (II) make the exporting or other-
24 wise observing of such intelligible in-
25 formation, or the cryptographic secret

1 used to protect such information, im-
2 possible; and

3 (iii) if the result of such processing of
4 the personal information is also personal
5 information, such result must be unintelli-
6 gible to the covered entity or service pro-
7 vider and protected by privacy-preserving
8 computing.

9 (B) INSUFFICIENT METHODOLOGIES.—The
10 Director may determine that a methodology of
11 privacy-preserving computing is insufficient for
12 the purposes of this definition.

13 (25) PROCESS.—The term “process” means to
14 perform or cause to be performed any operation or
15 set of operations on personal information or contents
16 of communication, whether or not by automated
17 means.

18 (26) PROTECTED CLASS.—The term “protected
19 class” means the actual or perceived race, color, eth-
20 nicity, national origin, religion, sex (including sexual
21 orientation and gender identity or expression), famil-
22 ial status, or disability of an individual or group of
23 individuals.

24 (27) PUBLICLY AVAILABLE INFORMATION.—
25 The term “publicly available information”—

1 (A) means—

2 (i) information that is lawfully made
3 available from a government entity;

4 (ii) information linked to a public in-
5 dividual or official that is made publicly
6 accessible, without restrictions on accessi-
7 bility other than the general authorization
8 to access the services used to make the in-
9 formation accessible; or

10 (iii) information of an individual
11 that—

12 (I) is made publicly accessible by
13 such individual, without restrictions
14 on accessibility other than the general
15 authorization to access the services
16 used to make the information acces-
17 sible; and

18 (II) such individual has the abil-
19 ity to delete or change without relying
20 on a request under section 102 or
21 103; and

22 (B) does not include—

23 (i) biometric information of an indi-
24 vidual collected by a covered entity without
25 the individual's knowledge;

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

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

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

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

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

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

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

3 (29) SELL AND SALE.—

4 (A) IN GENERAL.—The terms “sell” and
5 “sale” mean the disclosing of personal informa-
6 tion for monetary consideration or for a thing
7 of value by a covered entity to a third party for
8 the purposes of processing, maintaining or dis-
9 closing such personal information at the third
10 party’s discretion.

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

13 (i) the disclosing of personal informa-
14 tion of an individual to a third party with
15 which the individual has a direct relation-
16 ship for purposes of providing a product or
17 service requested by the individual or oth-
18 erwise in a manner that is consistent with
19 an individual’s reasonable expectations
20 considering the context in which the indi-
21 vidual provided the personal information to
22 the covered entity;

23 (ii) the disclosing or transfer of per-
24 sonal information to a subsidiary or an af-
25 filiate of the covered entity; or

1 (iii) the disclosing or transfer of per-
2 sonal information to a third party as an
3 asset that is part of a merger, acquisition,
4 bankruptcy, or other transaction in which
5 the third party assumes control of all or
6 part of the covered entity's assets, unless
7 personal information makes up the major-
8 ity of the value of the assets of which the
9 third party assumes control.

10 (30) SERVICE PROVIDER.—

11 (A) IN GENERAL.—The term “service pro-
12 vider” means a covered entity that—

13 (i) processes, discloses, or maintains
14 personal information, where such covered
15 entity does not process, disclose, or main-
16 tain the personal information other than in
17 accordance with the directions and on be-
18 half of another covered entity;

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

23 (iii) does not earn revenue from proc-
24 essing, maintaining, or disclosing personal
25 information disclosed to such covered enti-

1 ty by another covered entity except by pro-
2 viding contracted services to such other
3 covered entity;

4 (iv) does not disclose personal infor-
5 mation to another covered entity unless
6 such personal information was provided by
7 such other covered entity or resulted from
8 maintaining or processing performed on
9 personal information exclusively provided
10 by such other covered entity;

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

15 (vi) with respect to personal informa-
16 tion processed or maintained by such cov-
17 ered entity on behalf of another covered
18 entity, assists such other covered entity in
19 complying with title I, including providing
20 tools for such other covered entity to com-
21 ply with such requirements if requested;
22 and

23 (vii) does not link the personal infor-
24 mation provided by another covered entity

1 to personal information from any other
2 source.

3 (B) TREATMENT.—A covered entity shall
4 be treated as a service provider under this Act
5 only to the extent that such covered entity is
6 acting as a service provider, as defined in sub-
7 paragraph (A).

8 (31) SIGNIFICANT PRIVACY HARM.—The term
9 “significant privacy harm” means adverse con-
10 sequences to an individual arising from the col-
11 lecting, processing, maintaining, or disclosing of per-
12 sonal information or contents of communications,
13 limited to subparagraph (A), (B), or (D) of para-
14 graph (23).

15 (32) SMALL BUSINESS.—The term “small busi-
16 ness” means a covered entity that—

17 (A) does not earn revenue from the sale of
18 personal information;

19 (B) earns less than half of annual revenues
20 from the processing of personal information for
21 targeted or personalized advertising;

22 (C) has not, in combination with each sub-
23 sidiary and affiliate of the service, maintained
24 personal information of 250,000 or more indi-

1 viduals for 3 or more of the preceding 12
2 months;

3 (D) has fewer than 200 employees; and

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

7 (33) STATE.—The term “State” means each
8 State of the United States, the District of Columbia,
9 each commonwealth, territory, or possession of the
10 United States, and each federally recognized Indian
11 Tribe.

12 (34) STATE ATTORNEY GENERAL.—The term
13 “State attorney general” means, with respect to a
14 State, the attorney general or chief law enforcement
15 officer of the State, or another official or agency
16 designated by the State to bring civil actions on be-
17 half of the State or the residents of the State.

18 (35) STATE PRIVACY REGULATOR.—The term
19 “State privacy regulator” means an agency or in-
20 strumentality of a State that has the primary pur-
21 pose of administering, implementing, or enforcing a
22 privacy law or associated rules or regulations.

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

1 (A) to which such covered entity disclosed
2 personal information; and

3 (B) that is not—

4 (i) such covered entity;

5 (ii) a subsidiary or corporate affiliate
6 of such covered entity; or

7 (iii) a service provider of such covered
8 entity.

9 (37) USERS.—The term “users” means, with
10 respect to a product or service, the monthly active
11 users, subscribers, or customers (or a reasonable
12 proxy or substitute therefor determined by the Di-
13 rector) of such product or service.

14 (38) VIOLATION.—The term “violation” means,
15 except where otherwise specified, any act or omission
16 that, if proved, would constitute a violation of any
17 provision of this Act or a rule or order issued pursu-
18 ant to this Act.

19 **SEC. 3. GENERAL PROVISIONS.**

20 (a) RULES OF CONSTRUCTION WITH RESPECT TO
21 PERSONAL INFORMATION AND INDIVIDUALS.—In this
22 Act—

23 (1) any reference to information as being of or
24 belonging to an individual shall be construed to
25 mean that such information is linked or reasonably

1 linkable to such individual as described in section
2 2(21)(A); and

3 (2) any reference to any communication as
4 being of or belonging to an individual shall be con-
5 strued to mean that such individual is party to such
6 communication.

7 (b) PROHIBITION ON WAIVERS.—

8 (1) IN GENERAL.—The provisions under this
9 Act may not be waived. Any agreement purporting
10 to waive compliance with or modifying any provision
11 of this Act shall be void as contrary to public policy.

12 (2) PROHIBITION ON PREDISPUTE ARBITRATION
13 AGREEMENTS.—No predispute arbitration agreement
14 shall be valid or enforceable with respect to any
15 claims under this Act.

16 (c) JOURNALISM PROTECTION.—

17 (1) IN GENERAL.—Covered entities engaged in
18 journalism shall not be subject to the obligations im-
19 posed under this Act to the extent that those obliga-
20 tions directly infringe on the journalism rather than
21 the business practices of the covered entity, so long
22 as the covered entity has technical safeguards and
23 business processes that prevent the collecting, proc-
24 essing, maintaining, or disclosing of such personal

1 information for business practices other than jour-
2 nalism.

3 (2) JOURNALISM.—The term “journalism” in-
4 cludes the collecting, maintaining, processing, and
5 disclosing of personal information about a public in-
6 dividual or official, or that otherwise concerns mat-
7 ters of public interest, for dissemination to the pub-
8 lic.

9 (d) SMALL BUSINESS COMPLIANCE RAMP.—Upon
10 losing its status as a small business, a covered entity shall
11 have nine months to comply with provisions of this Act
12 that a small business is exempt from complying with.

13 (e) PROHIBITION ON COLLECTING, MAINTAINING,
14 PROCESSING, OR DISCLOSING PERSONAL INFORMA-
15 TION.—A covered entity may not collect, maintain, proc-
16 ess, or disclose personal information using a channel of
17 interstate commerce unless such covered entity is in com-
18 pliance with all requirements of this Act.

19 **SEC. 4. LIMITATION ON DISCLOSING NONREDACTED GOV-**
20 **ERNMENT RECORDS.**

21 (a) IN GENERAL.—A government entity may not use
22 a channel of interstate commerce to disclose the personal
23 information of an individual in a government record with-
24 out an agreement prohibiting the recipient of such infor-

1 mation from selling the information without the express
2 consent of the individual.

3 (b) EXCEPTION.—Notwithstanding subsection (a),
4 this section does not prohibit the disclosure of personal
5 information using a channel of interstate commerce to an-
6 other government entity without consent of the individual.

7 **SEC. 5. CRIMINAL PROHIBITION ON DOXXING.**

8 (a) IN GENERAL.—Chapter 41 of title 18, United
9 States Code, is amended by adding at the end the fol-
10 lowing:

11 **“§ 881. Disclosing of personal information with the**
12 **intent to cause harm**

13 “(a) IN GENERAL.—Whoever uses a channel of inter-
14 state or foreign commerce to knowingly disclose an indi-
15 vidual’s personal information with the intent—

16 “(1) to threaten, intimidate, or harass any per-
17 son, incite or facilitate the commission of a crime of
18 violence against any person, or place any person in
19 reasonable fear of death or serious bodily injury; or

20 “(2) that the information will be used to threat-
21 en, intimidate, or harass any person, incite or facili-
22 tate the commission of a crime of violence against
23 any person, or place any person in reasonable fear
24 of death or serious bodily injury,

1 shall be fined under this title or imprisoned not more than
2 5 years, or both.

3 “(b) DIGITAL PRIVACY AGENCY.—

4 “(1) SUPPORT FUNCTIONS.—The Director of
5 the Digital Privacy Agency may—

6 “(A) receive complaints and refer credible
7 complaints to the Attorney General;

8 “(B) coordinate with appropriate law en-
9 forcement agencies to support investigations;
10 and

11 “(C) provide technical assistance upon the
12 request of the Attorney General.

13 “(2) RULE OF CONSTRUCTION.—Nothing in
14 this section shall be construed to authorize the Dig-
15 ital Privacy Agency to prosecute an offense under
16 this section.

17 “(c) DEFINITIONS.—In this section:

18 “(1) CONTENTS.—The term ‘contents’ when
19 used with respect to communication, has the mean-
20 ing given such term in section 2510 of this title.

21 “(2) DISCLOSE.—The term ‘disclose’ means,
22 with respect to personal information or contents of
23 communication, to sell, release, transfer, share, dis-
24 seminate, make available, or otherwise cause to be

1 communicated such information or contents to a
2 third party.

3 “(3) GOVERNMENT ENTITY.—The term ‘gov-
4 ernment entity’ means—

5 “(A) a Federal agency (as that term is de-
6 fined in section 3371 of title 5);

7 “(B) a State or political subdivision there-
8 of; or

9 “(C) any agency, authority, or instrumen-
10 tality of a State or political subdivision thereof.

11 “(4) INDIVIDUAL.—The term ‘individual’ means
12 a natural person residing in the United States.

13 “(5) PERSONAL INFORMATION.—

14 “(A) IN GENERAL.—The term ‘personal in-
15 formation’ means any information maintained
16 by a person that, on its own or combined with
17 other information, is linked or reasonably
18 linkable to a specific individual.

19 “(B) EXCLUSIONS.—The term ‘personal
20 information’ does not include—

21 “(i) publicly available information
22 linked to an individual; or

23 “(ii) information derived or inferred
24 from personal information, if the derived

1 or inferred information is not linked or
2 reasonably linkable to a specific individual.

3 “(6) PUBLICLY AVAILABLE INFORMATION.—

4 The term ‘publicly available information’—

5 “(A) means—

6 “(i) information that is lawfully made
7 available from a government entity;

8 “(ii) information linked to a public in-
9 dividual or official that is made publicly
10 accessible, without restrictions on accessi-
11 bility other than the general authorization
12 to access the services used to make the in-
13 formation accessible; or

14 “(iii) information of an individual
15 that—

16 “(I) is made publicly accessible
17 by such individual, without restric-
18 tions on accessibility other than the
19 general authorization to access the
20 services used to make the information
21 accessible; and

22 “(II) such individual has the abil-
23 ity to delete or change; and

24 “(B) does not include—

1 “(i) biometric information of an indi-
2 vidual collected by a covered entity without
3 the individual’s knowledge;

4 “(ii) information used for a purpose
5 that is not compatible with the purpose for
6 which the information is maintained and
7 made available in government records;

8 “(iii) information obtained from gov-
9 ernment records for the purpose of selling
10 such information; or

11 “(iv) information used to contact or
12 locate a private individual either physically
13 or electronically.

14 “(7) STATE.—The term ‘State’ means each
15 State of the United States, the District of Columbia,
16 each commonwealth, territory, or possession of the
17 United States, and each federally recognized Indian
18 Tribe.”.

19 (b) CLERICAL AMENDMENT.—The table of sections
20 for chapter 41 of title 18, United States Code, is amended
21 by inserting after the item relating to section 880 the fol-
22 lowing:

“881. Disclosing of personal information with the intent to cause harm.”.

1 **TITLE I—INDIVIDUAL RIGHTS**

2 **SEC. 101. RIGHT OF ACCESS.**

3 (a) IN GENERAL.—A covered entity shall make avail-
4 able a reasonable mechanism by which an individual may
5 access—

6 (1) the categories of personal information and
7 contents of communications of such individual that
8 is maintained by such covered entity, including, in
9 the case of personal information that such covered
10 entity did not collect from such individual, how and
11 from whom such covered entity obtained such per-
12 sonal information;

13 (2) a list of the third parties, subsidiaries, and
14 corporate affiliates, to which such covered entity has
15 disclosed and from which such covered entity has, at
16 any time on or after the effective date of this Act,
17 obtained the personal information of such individual;

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

21 (A) for collecting, processing, or maintain-
22 ing the personal information of such individual;
23 and

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

1 (4) a list of automated decision-making proc-
2 esses that an individual has a right to request
3 human review of under section 105 with a concise
4 and clear description of the implications and in-
5 tended effects of each such process.

6 (b) EXCEPTION FOR PUBLICLY ACCESSIBLE INFOR-
7 MATION.—A covered entity that makes available informa-
8 tion required in subsection (a) shall be considered in com-
9 pliance with such requirements if the covered entity pro-
10 vides an individual with instructions on how to access a
11 public posting of such information, including in a privacy
12 policy, if the instructions are easy and do not require pay-
13 ment.

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

16 **SEC. 102. RIGHT OF CORRECTION.**

17 (a) DISPUTE BY INDIVIDUAL.—A covered entity shall
18 make available a reasonable mechanism by which an indi-
19 vidual may dispute the accuracy or completeness of per-
20 sonal information linked to such individual that is main-
21 tained by such covered entity if such information is proc-
22 essed in any way, by such covered entity, a third party
23 of such covered entity, or a service provider of such cov-
24 ered entity that may increase reasonably foreseeable sig-
25 nificant privacy harms.

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

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

6 (2) notify such individual that—

7 (A) the disputed information is correct or
8 complete;

9 (B) such covered entity lacks sufficient in-
10 formation to correct or complete the disputed
11 information; or

12 (C) such covered entity is denying the re-
13 quest for correction or completion in reliance on
14 an exemption or exception provided by section
15 109(g).

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

18 **SEC. 103. RIGHT OF DELETION.**

19 (a) REQUEST BY INDIVIDUAL.—A covered entity
20 shall make available a reasonable mechanism by which an
21 individual may request the deletion of personal informa-
22 tion and contents of communications of such individual
23 maintained by such covered entity, including any such in-
24 formation that such covered entity acquired from a third

1 party or inferred from other information maintained by
 2 such covered entity.

3 (b) DELETION BY COVERED ENTITY.—A covered en-
 4 tity receiving a request for deletion under subsection (a)
 5 shall—

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

8 (2) notify such individual that such covered en-
 9 tity is denying the request for deletion in reliance on
 10 an exemption or exception provided by section
 11 109(g).

12 **SEC. 104. RIGHT OF PORTABILITY.**

13 (a) DETERMINATION OF PORTABLE CATEGORIES.—

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

17 (A) establish categories of products and
 18 services offered by covered entities, based on
 19 similarities in the products and services;

20 (B) determine which categories established
 21 under subparagraph (A) are portable categories;
 22 and

23 (C) publish in the Federal Register a list
 24 of portable categories determined under sub-
 25 paragraph (B).

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

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

6 (B) provide an opportunity for public com-
7 ment on such draft list.

8 (b) EXERCISE OF RIGHT.—

9 (1) IN GENERAL.—A covered entity that offers
10 a product or service in a portable category and that
11 maintains personal information or the contents of
12 any communications of an individual shall make
13 available to such individual a reasonable mechanism
14 by which such individual may—

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

17 (i) any such personal information that
18 such individual has provided to such cov-
19 ered entity, with the option to download
20 such information by category that is acces-
21 sible under section 101; and

22 (ii) the contents of any such commu-
23 nications; and

24 (B) using a real-time application program-
25 ming interface, or similar mechanism, transmit

1 all such personal information (whether or not
2 provided to such covered entity by such indi-
3 vidual) and the contents of any such commu-
4 nication from such covered entity to another
5 covered entity in accordance with subsection
6 (c).

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

11 (A) be publicly documented;

12 (B) allow the option of obtaining any per-
13 sonal information of an individual that the indi-
14 vidual has provided to the covered entity, if
15 such information is accessible under section
16 101;

17 (C) include a publicly available, fully func-
18 tional test version for development purposes;
19 and

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

22 (c) REQUIREMENTS FOR ACCESS TO AN APPLICATION
23 PROGRAMMING INTERFACE.—

24 (1) ACCESS.—Except as provided in paragraph

25 (2)(A), a covered entity shall provide access to the

1 application programming interface or similar mecha-
2 nism required by subsection (b)(1)(B) upon the re-
3 quest of another covered entity if the requesting cov-
4 ered entity has self-certified, using the procedures
5 established by the Director under paragraph (3)(A),
6 that such requesting covered entity—

7 (A) is a covered entity;

8 (B) can have personal information dis-
9 closed to it under section 204;

10 (C) is, at the time of the self-certification,
11 in compliance with all applicable requirements
12 of this Act (including provisions a small busi-
13 ness is otherwise exempt from complying with);

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

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

19 (2) DENIAL OF ACCESS.—

20 (A) IN GENERAL.—A covered entity may
21 deny access to the application programming
22 interface or similar mechanism required by sub-
23 section (b)(1)(B) if such covered entity has an
24 objective, reasonable belief that the requesting

1 covered entity has failed to meet the require-
2 ments for self-certification under paragraph (1).

3 (B) REVIEW.—In accordance with the pro-
4 cedures established under paragraph (3)(B), a
5 covered entity the request of which is denied
6 under subparagraph (A) may petition the Di-
7 rector for review of the denial. If the Director
8 finds that such denial is unreasonable, the Di-
9 rector shall impose a penalty, to be established
10 in such procedures, on the covered entity that
11 denied the request.

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

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

16 (B) procedures for the review of petitions
17 under paragraph (2)(B), including penalties for
18 unreasonable denials.

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

21 (e) PORTABLE CATEGORY DEFINED.—In this sec-
22 tion, the term “portable category” means a category of
23 products and services established by the Director under
24 subsection (a)(1)(A)—

1 (1) for which the sum obtained by adding the
2 number of users or estimated users of each product
3 or service in such category is greater than
4 10,000,000; and

5 (2) that—

6 (A) has an estimated Herfindahl-
7 Hirschman Index of 2,000 or greater;

8 (B) has 3 or fewer covered entities offering
9 products and services in such category; or

10 (C) the Director otherwise determines that
11 a category would benefit from encouraging in-
12 creased competition.

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

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

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

22 (2) make available a reasonable mechanism by
23 which such individual may request human review of
24 such decision, upon request or in a publicly acces-
25 sible location; and

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

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

5 (a) IN GENERAL.—A covered entity may not, without
6 the affirmative express consent of an individual, collect,
7 process, maintain, or disclose the personal information of
8 the individual to create, improve upon, maintain, process,
9 or otherwise link the individual with an algorithm, model,
10 or other means designed for behavioral personalization.

11 (b) CONSENT.—

12 (1) CONSENT REQUIRED.—A covered entity
13 shall obtain express affirmative consent from an in-
14 dividual before the entity provides a behaviorally
15 personalized version of a product or service, and not
16 less than every calendar year thereafter.

17 (2) DENIAL OF CONSENT.—For a case in which
18 consent is denied, the covered entity shall provide
19 the product or service without behavioral personal-
20 ization, except as provided in subsection (c).

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

23 (1) INFEASIBILITY.—For a case in which the
24 offering of a substantially similar product or service
25 without behavioral personalization is infeasible, a

1 covered entity shall provide, to the greatest extent
2 feasible, a core aspect or part of the product or serv-
3 ice that can be offered without behavioral personal-
4 ization.

5 (2) DENIAL FOR INABILITY TO FUNCTION.—

6 For a case in which a core aspect or part of the
7 product or service is not able to function in a sub-
8 stantially similar function without behavioral person-
9 alization, a covered entity may deny providing an in-
10 dividual use of such product or service if such indi-
11 vidual does not consent to behavioral personalization
12 as required in subsection (a).

13 (d) EXCEPTION TO BEHAVIORAL PROCESSING.—Not-
14 withstanding subsections (a) and (b), a covered entity may
15 process personal information to create or operate behav-
16 ioral personalization algorithms, models, or other mecha-
17 nisms for the purpose of increasing the usability of the
18 product or service provided by a covered entity that—

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

22 (2) have an output that is both uniform across
23 the individuals that use the product or service and
24 independent of a specific individual's inherent or be-
25 havioral characteristics.

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

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

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

10 A covered entity that collects personal information of
11 an individual with whom such covered entity does not have
12 an existing relationship (as of the time of the collecting),
13 if such personal information includes contact information,
14 shall notify such individual within 30 days after receipt
15 of such information, in writing if possible and at no charge
16 to the individual, that such covered entity has collected
17 the personal information of such individual.

18 **SEC. 108. RIGHT TO IMPERMANENCE.**

19 (a) LIMITATION ON MAINTAINING OF PERSONAL IN-
20 FORMATION.—A covered entity may not maintain personal
21 information for more time than expressly consented to by
22 an individual whose personal information is being main-
23 tained.

24 (b) CONSENT.—A covered entity shall obtain express
25 affirmative consent from an individual before maintaining

1 the personal information of such individual for any dura-
2 tion. Such consent may be obtained for categories of per-
3 sonal information and shall give an individual options to
4 affirmatively choose granting a covered entity consent for
5 various durations, at least including—

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

10 (2) until consent is revoked; and

11 (3) one or more additional durations based on
12 reasonable expectations and norms for maintaining
13 the category of personal information.

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

20 **SEC. 109. ADDITIONAL RIGHTS AND EXCEPTIONS.**

21 (a) IN GENERAL.—The Director may, by rule and
22 subject to notice and comment, establish procedural re-
23 quirements and narrowly tailored exceptions governing the
24 exercise of rights under this title, limited to the following:

1 (1) Identity verification and authentication pro-
2 cedures.

3 (2) Standardized formats and reasonable mech-
4 anisms for submitting and fulfilling requests.

5 (3) Reasonable limits to prevent fraud, abuse,
6 or excessive and duplicative requests.

7 (4) Timelines and recordkeeping requirements
8 consistent with this title.

9 (5) Narrowly tailored exceptions necessary to
10 prevent a legitimate risk to the privacy, security, or
11 safety of another individual, or to protect free ex-
12 pression, consistent with section 110(b).

13 (b) LIMITATIONS.—The Director may not create any
14 new substantive right or broadly waive compliance with
15 this title.

16 **SEC. 110. EXEMPTIONS, EXCEPTIONS, FEES, TIMELINES,**
17 **AND RULES OF CONSTRUCTION FOR RIGHTS**
18 **UNDER THIS TITLE.**

19 (a) EXEMPTIONS FOR PERSONAL INFORMATION FOR
20 PARTICULAR PURPOSES.—

21 (1) IN GENERAL.—This title does not apply
22 with respect to personal information that is col-
23 lected, processed, maintained, or disclosed for any of
24 the following purposes (or a combination of such
25 purposes), where a covered entity has technical safe-

1 guards and business processes that limit collecting,
2 processing, maintaining, or disclosing of such per-
3 sonal information to the following purposes:

4 (A) Detecting, responding to, or preventing
5 security incidents or threats.

6 (B) Protecting against malicious, decep-
7 tive, fraudulent, or illegal activity.

8 (C) A good faith response to, or compli-
9 ance with, a valid subpoena, court order, or
10 warrant (including a subpoena and court order
11 obtained by an entity that is not a government
12 entity) or otherwise providing information as
13 required by law.

14 (D) Protecting a legally recognized privi-
15 lege or other legal right.

16 (E) Protecting public safety.

17 (F) Collecting, processing, or maintaining
18 by an employer pursuant to an employer-em-
19 ployee relationship of records about employees
20 or employment status, except—

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

1 (ii) was disclosed to the employer by
2 a third party.

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

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

10 (I) Providing transparency in advertising
11 or origination of user-generated content.

12 (2) RE-IDENTIFICATION.—Where compliance
13 with this title would require the re-identification of
14 de-identified personal information, and the covered
15 entity does not already maintain the information
16 necessary for such re-identification, the covered enti-
17 ty shall be exempt from such compliance, except for
18 requirements under section 106.

19 (3) DISCLOSING.—A covered entity relying on
20 an exemption under paragraph (1) with respect to
21 personal information shall disclose in the privacy
22 policy maintained by such entity under section
23 211—

1 (A) the reason for which such information
2 is collected, processed, maintained, or disclosed;
3 and

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

8 (b) EXCEPTIONS FOR PARTICULAR REQUESTS.—

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

11 (A) such covered entity cannot confirm the
12 identity of such individual;

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

17 (C) such covered entity determines that
18 granting the request of such individual would
19 create a legitimate risk to free expression; or

20 (D) the personal information requested to
21 be corrected under section 102 or deleted under
22 section 103—

23 (i) is necessary to the completion of a
24 transaction initiated before such request

1 was made or the performance of a contract
2 entered into before such request was made;

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

6 (iii) would undermine the integrity of
7 a legally significant transaction.

8 (2) LIMITATIONS ON REQUESTS FOR ADDI-
9 TIONAL INFORMATION TO CONFIRM IDENTITY.—A

10 covered entity may not deny a request of an indi-
11 vidual under paragraph (1)(A) on the basis of the
12 refusal of such individual to provide additional per-
13 sonal information to such covered entity to confirm
14 the identity of such individual—

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

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

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

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

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

11 (1) comply with such request; or

12 (2) inform such individual of the reason for de-
13 nying such request, as allowed under subsection (a)
14 or (b).

15 (f) FEES PROHIBITED.—

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

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

24 (3) AGENCY NOTICE.—If a covered entity plans
25 to charge a fee under paragraph (2), it must notify

1 the Digital Privacy Agency at least 7 days before
2 charging such fee.

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

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

9 (B) such request is not unfounded or ex-
10 cessive.

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

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

16 (2) collect or maintain personal information or
17 contents of communication that the covered entity
18 would otherwise not maintain (including a record of
19 an individual exercising rights under this title); or

20 (3) maintain personal information or contents
21 of communication longer than the covered entity
22 would otherwise maintain such personal information.

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

5 **SEC. 201. MINIMIZATION.**

6 (a) **ARTICULATED BASIS.**—A covered entity shall
7 have a reasonable, articulated basis for collecting, proc-
8 essing, maintaining, and disclosing of personal informa-
9 tion that takes into account the reasonable business needs
10 of the covered entity and minimum amount of personal
11 information necessary for providing the service, balanced
12 with the intrusion on the privacy of, potential privacy
13 harms to, and reasonable expectations of individuals to
14 whom the personal information relates.

15 (b) **MINIMIZATION OF COLLECTING, PROCESSING,**
16 **MAINTAINING, AND DISCLOSING.**—

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

21 (2) **PROCESSING.**—A covered entity may not
22 process personal information for a purpose other
23 than the purpose for which such information was
24 originally collected from the individual or in the case
25 of a service provider, a purpose other than that

1 which is in accordance with the directions of a cov-
2 ered entity.

3 (3) MAINTAINING.—A covered entity may not
4 maintain personal information once such information
5 is no longer needed for the purpose for which such
6 information was originally collected from the indi-
7 vidual or in the case of a service provider, a purpose
8 other than that which is in accordance with the di-
9 rections of a covered entity.

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

17 (c) ANCILLARY COLLECTING, PROCESSING, MAIN-
18 TAINING, AND DISCLOSING.—Notwithstanding subsection
19 (b), a covered entity may collect, process, disclose, or
20 maintain personal information beyond limitations under
21 subsection (b) only if such covered entity complies with
22 this subsection.

23 (1) NO NOTICE OR CONSENT REQUIRED.—A
24 covered entity may collect, process, or maintain per-
25 sonal information without additional notice or con-

1 sent if the purpose for such collecting, processing, or
2 maintaining is substantially similar to the type of
3 personal information and purpose for which such
4 personal information was originally collected and
5 such ancillary collecting, processing, or maintaining
6 will not result in additional or increased privacy
7 harms.

8 (2) NOTICE REQUIRED.—A covered entity shall
9 provide notice of ancillary collecting, processing,
10 maintaining, or disclosing of personal information in
11 the case of one, but not more than one, of the fol-
12 lowing instances:

13 (A) Such ancillary collecting, processing,
14 maintaining, or disclosing may result in addi-
15 tional or increased privacy harms (but not in-
16 creased significant privacy harms), and is sub-
17 stantially similar to the purpose for which such
18 personal information was originally collected.

19 (B) Such ancillary collecting, processing,
20 maintaining, or disclosing is not substantially
21 similar to the purpose for which such personal
22 information was originally collected, but will not
23 result in additional or increased privacy harms.

24 (C) Such ancillary collecting, processing,
25 maintaining, or disclosing may result in addi-

1 tional or increased privacy harms (but not in-
2 creased significant privacy harms), and the pur-
3 pose is not substantially similar to the purpose
4 for which such personal information was origi-
5 nally collected, so long as the personal informa-
6 tion is secured using privacy-preserving com-
7 puting.

8 (3) NOTICE AND CONSENT REQUIRED.—For
9 scenarios not covered under paragraph (1) or (2),
10 and notwithstanding sections 208(b)(2) and (3), a
11 covered entity shall provide notice of and obtain con-
12 sent for ancillary collecting, processing, maintaining,
13 or disclosing of personal information.

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

21 **SEC. 202. MINIMIZATION AND RECORDS OF ACCESS BY EM-**
22 **PLOYEES AND CONTRACTORS.**

23 (a) MINIMIZATION.—A covered entity shall restrict
24 access to personal information and contents of commu-
25 nications by the employees or contractors of such covered

1 entity based on an articulated balance between the poten-
2 tial for privacy harm, reasonable expectations of individ-
3 uals to whom the personal information relates, and reason-
4 able business needs.

5 (b) RECORDS OF ACCESS.—

6 (1) IN GENERAL.—A covered entity shall main-
7 tain records identifying each instance in which an
8 employee or a contractor of such covered entity ac-
9 cesses personal information or contents of commu-
10 nications if disclosing such personal information or
11 contents of communication, or a data breach or
12 data-sharing abuse involving such personal informa-
13 tion or contents of communication, may foreseeably
14 result in increased privacy harms.

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

17 (A) A unique identifier for the employee or
18 contractor accessing personal information or
19 contents of communications.

20 (B) The date and time of access.

21 (C) The fields of information accessed.

22 (D) The individuals whose personal infor-
23 mation was accessed or the contents of whose
24 communications were accessed.

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

3 **SEC. 203. PROHIBITIONS ON DISCLOSING OF PERSONAL IN-**
4 **FORMATION.**

5 (a) CONSENT FOR DISCLOSING REQUIRED.—

6 (1) IN GENERAL.—A covered entity may not in-
7 tentionally disclose personal information unless the
8 covered entity obtains consent of the individual
9 whose personal information is being disclosed for
10 each category of third party to which such personal
11 information will be disclosed. Such covered entity
12 must also provide such individual with notice of—

13 (A) each category of third party;

14 (B) the personal information to be dis-
15 closed; and

16 (C) a concise and clear description of the
17 business or commercial purpose for disclosing
18 such personal information.

19 (2) ADDITIONAL REQUIREMENTS FOR SALE OF
20 PERSONAL INFORMATION.—

21 (A) IN GENERAL.—A covered entity may
22 not intentionally sell personal information un-
23 less the covered entity—

1 (i) obtains the consent required by
2 paragraph (1) for disclosing such personal
3 information; and

4 (ii) provides the individual to whom
5 such personal information relates with the
6 identity of the specific third party to which
7 such personal information will be disclosed.

8 (B) DISCLOSING SERVICES.—Subpara-
9 graph (A) shall not apply to a covered entity in
10 a case in which an individual is directing the
11 covered entity to disclose the personal informa-
12 tion of such individual for the sole purpose of
13 procuring goods or services, or offers for goods
14 or services, for such individual, if there is a rea-
15 sonable mechanism for the individual to with-
16 draw consent.

17 (3) REQUIREMENT TO INCLUDE ORIGINAL PUR-
18 POSE OF COLLECTING.—A covered entity may not
19 intentionally disclose personal information without
20 including the purpose for which the personal infor-
21 mation was originally collected.

22 (4) EXCEPTION FOR PRIVACY-PRESERVING
23 COMPUTING.—Notwithstanding paragraph (1), con-
24 sent is not required for disclosing (not including sell-

1 ing) personal information secured using privacy-pre-
2 serving computing.

3 (5) EXCEPTION FOR DE-IDENTIFIED PERSONAL
4 INFORMATION.—Notwithstanding paragraph (1),
5 consent is not required for disclosing (not including
6 selling) de-identified personal information where the
7 disclosed personal information is limited to the nar-
8 rowest possible scope likely to yield the intended
9 benefit and contractual obligations are in place that
10 prohibit—

11 (A) re-identification of the disclosed per-
12 sonal information; and

13 (B) the processing of additional personal
14 information in combination with the disclosed
15 personal information that would allow for the
16 re-identification of the disclosed personal infor-
17 mation.

18 (b) DISCLOSING FOR ADVERTISING OR MARKETING
19 PURPOSES.—

20 (1) IN GENERAL.—A covered entity may not in-
21 tentiously disclose for advertising or marketing pur-
22 poses a unique identifier or any other personal infor-
23 mation that would allow information disclosed to be
24 linked to information relating to the same individual
25 or device disclosed in the past.

1 (2) TREATMENT OF CERTAIN TYPES OF INFOR-
2 MATION.—Disclosing personal information or con-
3 tents of communication for advertising or marketing
4 purposes may not be treated as violating paragraph
5 (1) by reason of including any or all of the following:

6 (A) Internet Protocol addresses truncated
7 to no more than the first 24 bits for Internet
8 Protocol version 4 and the first 48 bits for
9 Internet Protocol version 6, or for a successor
10 protocol truncated to limit the precision of the
11 identifier to a network address of the internet
12 access provider.

13 (B) Geolocation information truncated to
14 allow no more than the equivalent of two dec-
15 imal degrees of precision at the equator or
16 prime meridian, or an equivalent precision in
17 another geolocation standard.

18 (C) A general description of a device,
19 browser, or operating system, or any combina-
20 tion thereof.

21 (D) An identifier that is unique to a dislo-
22 sure.

1 **SEC. 204. DISCLOSING TO ENTITIES NOT SUBJECT TO**
2 **UNITED STATES JURISDICTION OR NOT COM-**
3 **PLIANT WITH THIS ACT.**

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

6 (1) is not subject to the jurisdiction of the
7 United States; or

8 (2) is not in compliance with all requirements
9 of this Act.

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

18 (c) SAFE HARBORS FOR DISCLOSING.—Notwith-
19 standing subsection (a), a covered entity may disclose per-
20 sonal information to another covered entity (the receiving
21 covered entity) that is not subject to the jurisdiction of
22 the United States if either—

23 (1) the receiving covered entity has entered into
24 an agreement, as described in subsection (e), with
25 the Digital Privacy Agency, and—

1 (A) the covered entity has a reasonable be-
2 lief that the receiving covered entity is suffi-
3 ciently solvent to compensate victims or pay
4 fines for violations of this Act;

5 (B) a contract between the covered entity
6 and receiving covered entity requires that the
7 receiving covered entity complies with this Act,
8 and the covered entity has reason to believe the
9 receiving covered entity is compliant with this
10 Act; and

11 (C) a contract between the covered entity
12 and the receiving covered entity prohibits the
13 receiving covered entity from using the dis-
14 closed personal information for any purpose
15 other than provided in the contract; or

16 (2) the covered entity has—

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

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

21 (ii) prohibits the receiving covered en-
22 tity from using the disclosed personal in-
23 formation for any purpose other than pro-
24 vided in the contract;

1 (iii) requires the receiving covered en-
2 tity to indemnify the covered entity against
3 violations of this Act committed by the re-
4 ceiving covered entity for any amount the
5 covered entity is unable to pay of a judg-
6 ment for such violation;

7 (iv) grants the covered entity the au-
8 thority to audit, including physical access
9 to electronic devices and data, the receiving
10 covered entity's compliance with this Act
11 and the contract; and

12 (v) requires the receiving covered enti-
13 ty to assist the covered entity in respond-
14 ing to and complying with any court or-
15 ders, Digital Privacy Agency orders, or the
16 exercising of an individual's rights under
17 this Act;

18 (B) actual knowledge that the receiving
19 covered entity is in compliance with this Act
20 and not using personal information contrary to
21 their agreement;

22 (C) actual knowledge that the receiving
23 covered entity is sufficiently solvent to com-
24 pensate victims or pay fines for violations of
25 this Act;

1 (D) an auditing and compliance program
2 to ensure the receiving covered entity's contin-
3 ued compliance with this Act and contract
4 terms;

5 (E) filed with the Digital Privacy Agency
6 the terms of said contract, proof of its actual
7 knowledge of the receiving covered entity's com-
8 pliance with this Act and contract terms, and
9 documents detailing its auditing and compliance
10 program for approval and publication by the
11 Digital Privacy Agency; and

12 (F) entered into an agreement with the
13 Digital Privacy Agency where the covered entity
14 agrees to accept, respond to, or comply with a
15 court order, Digital Privacy Agency order, or
16 request by an individual regarding actions
17 taken by the receiving covered entity with re-
18 spect to covered information it has disclosed.

19 (d) LIABILITY FOR VIOLATION BY RECEIVING COV-
20 ERED ENTITY; FAILURE TO REPORT.—For the purposes
21 of subsection (c)(2), the covered entity shall be jointly lia-
22 ble for a violation of this Act by the receiving covered enti-
23 ty regarding the personal information the covered entity
24 disclosed, except where the covered entity was the first to
25 notify the Digital Privacy Agency of the violation, in which

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

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

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

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

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

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

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

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

12 (7) A default judgment, failure to comply with
13 Digital Privacy Agency investigative requests or or-
14 ders, or failure to comply with United States court
15 orders or decisions shall result in the immediate ter-
16 mination of the agreement.

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

1 **SEC. 205. PROHIBITION ON RE-IDENTIFICATION.**

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

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

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

14 **SEC. 206. RESTRICTIONS ON COLLECTING, PROCESSING,**
15 **MAINTAINING, AND DISCLOSING CONTENTS**
16 **OF COMMUNICATIONS.**

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

22 (1) transmitting or displaying the communica-
23 tion to any intended recipient or the original sender,
24 or maintaining such communications for such pur-
25 poses;

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

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

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

9 (5) disclosing otherwise required by law;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16 **SEC. 207. PROHIBITION ON DISCRIMINATORY PROCESSING.**

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

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

8 (c) DISPARATE IMPACT AUTHORITY.—Not later than
9 6 months after the date of the enactment of this Act, the
10 Director shall issue additional requirements related to a
11 disparate impact standard that—

12 (1) describes other circumstances in which an
13 individual or group of individuals may be harmed by
14 an action of a covered entity through the processing
15 of personal information or contents of communica-
16 tion of the protected class status of that individual
17 in a manner not described in subsection (a) or (b);

18 (2) prohibits such action; and

19 (3) provides for enforcement under this Act or
20 through regulation.

21 (d) REGULATIONS.—Not later than one year after the
22 date of the enactment of this Act, the Director shall pro-
23 mulgate regulations to implement this section and may de-
24 fine any term used under this section, including “discrimi-

1 nates against” and “otherwise makes opportunities un-
2 available”.

3 **SEC. 208. REQUIREMENTS FOR NOTICE AND CONSENT**
4 **PROCESSES AND PRIVACY POLICIES.**

5 (a) MINIMUM THRESHOLD.—The Director shall es-
6 tablish minimum thresholds that covered entities must
7 meet for the percentage of individuals who understand a
8 notice or consent process or privacy policy required by this
9 Act. In establishing such minimum thresholds, the Direc-
10 tor shall—

11 (1) vary required thresholds on types and scale
12 of reasonably foreseeable privacy harms; and

13 (2) take into account expectations of individ-
14 uals, potential privacy harms, and individuals’
15 awareness of privacy harms.

16 (b) CONSENT REVOCATION.—A covered entity shall
17 make available a reasonable mechanism by which an indi-
18 vidual may revoke consent for any consent given under
19 this Act.

20 (c) SAFE HARBOR.—

21 (1) APPROVAL PROCEDURES.—The Director
22 shall develop procedures for analyzing and approving
23 data submitted by a covered entity to establish that
24 a notice and consent process or privacy policy of

1 such covered entity meets the threshold established
2 under subsection (a).

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

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

18 (4) SMALL BUSINESS ADOPTION OF NOTICE OR
19 CONSENT PROCESS OF ANOTHER COVERED ENTI-
20 TY.—

21 (A) IN GENERAL.—If a small business
22 adopts a notice or consent process of another
23 covered entity that collects, processes, main-
24 tains, or discloses personal information in sub-
25 stantially the same way as such small business,

1 if the process of such other covered entity has
2 been approved under paragraph (1), the process
3 of such small business shall receive the pre-
4 sumption under paragraph (2).

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

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

1 (D) INAPPLICABILITY TO PRIVACY POL-
2 ICY.—Paragraph (4) does not apply with re-
3 spect to a privacy policy.

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

10 **SEC. 209. PROHIBITION ON “DARK PATTERNS” IN NOTICE**
11 **AND CONSENT PROCESSES AND PRIVACY**
12 **POLICIES.**

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

18 (1) understand the contents of such notice or
19 such privacy policy;

20 (2) understand the process for granting such
21 consent;

22 (3) make a decision regarding whether to grant
23 or withdraw such consent; or

24 (4) act on any such decision.

1 **SEC. 210. NOTICE AND CONSENT REQUIRED.**

2 (a) NOTICE.—A covered entity shall provide an indi-
3 vidual with notice of the personal information such covered
4 entity collects, processes, maintains, and discloses through
5 a process that is concise and clear and can be objectively
6 shown to meet the threshold established by the Director
7 under section 208(a).

8 (b) CONSENT.—

9 (1) EXPRESS CONSENT REQUIRED.—Except as
10 provided in paragraphs (2) and (3), a covered entity
11 may not collect from an individual personal informa-
12 tion that creates or increases the risk of foreseeable
13 privacy harms, or process or maintain any such per-
14 sonal information collected from an individual, un-
15 less such entity obtains the express consent of such
16 individual to the collecting, processing, or maintain-
17 ing (or any combination thereof) of such information
18 through a process that is concise and clear and can
19 be objectively shown to meet the threshold estab-
20 lished by the Director under section 208(a).

21 (2) EXCEPTION FOR IMPLIED CONSENT.—Not-
22 withstanding paragraph (1), express consent is not
23 required for collecting, processing, or maintaining
24 personal information if the collecting, processing, or
25 maintaining is, on its face, obvious and necessary to
26 provide a service at the request of the individual and

1 the personal information is collected, processed, or
2 maintained only for such request. Nothing in this
3 paragraph shall be construed to exempt the covered
4 entity from the requirement of subsection (a) to pro-
5 vide notice to such individual with respect to such
6 collecting, processing, or maintaining.

7 (3) EXEMPTION FOR PRIVACY-PRESERVING
8 COMPUTING.—Notwithstanding paragraph (1), ex-
9 cept with regard to consent for purposes of section
10 106, express consent is not required for collecting,
11 processing, or maintaining personal information se-
12 cured using privacy-preserving computing. Nothing
13 in this paragraph shall be construed to exempt the
14 covered entity from the requirement of subsection
15 (a) to provide notice to such individual with respect
16 to such collecting, processing, or maintaining.

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

22 **SEC. 211. PRIVACY POLICY.**

23 (a) POLICY REQUIRED.—A covered entity shall main-
24 tain a privacy policy relating to the practices of such entity

1 regarding the collecting, processing, maintaining, and dis-
2 closing of personal information.

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

5 (1) A general description of the practices of the
6 covered entity regarding the collecting, processing,
7 maintaining, and disclosing of personal information.

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

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

12 (A) The categories of personal information
13 collected or otherwise obtained by the covered
14 entity.

15 (B) The business or commercial purposes
16 of the covered entity for collecting, processing,
17 maintaining, or disclosing personal information.

18 (C) The categories and a list of third par-
19 ties to which the covered entity discloses per-
20 sonal information.

21 (4) A description of the personal information
22 that the covered entity maintains that the covered
23 entity does not collect from individuals and how the
24 covered entity obtains such personal information.

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

3 (6) A list of the third parties from which the
4 covered entity has obtained personal information at
5 any time on or after the effective date of this Act.

6 (7) The articulated basis for the collecting,
7 processing, disclosing, and maintaining of personal
8 information, as required under section 201(a).

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

17 (d) AVAILABILITY OF PRIVACY POLICY.—

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

20 (A) clear and in plain language; and

21 (B) made publicly available in a prominent
22 location on an ongoing basis.

23 (2) TIMING.—The privacy policy required by
24 subsection (a) shall be made available as required by

1 paragraph (1) before the covered entity collects per-
2 sonal information after the effective date of this Act.

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

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

10 **SEC. 212. INFORMATION SECURITY REQUIREMENTS.**

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

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

18 (2) the sensitivity of any personal information
19 at issue;

20 (3) the current state of the art in administra-
21 tive, technical, and physical safeguards for pro-
22 tecting such information; and

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

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

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

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

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

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

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

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

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

17 (c) REGULATIONS.—The Director, in consultation
18 with the Cybersecurity and Infrastructure Security Agen-
19 cy and the National Institute of Standards and Tech-
20 nology, shall promulgate regulations to implement this
21 section.

22 (d) SMALL BUSINESSES ASSISTANCE.—The Director,
23 in consultation with the Cybersecurity and Infrastructure
24 Security Agency, the National Institute of Standards and
25 Technology, the Small Business Administration, the Mi-

1 nority Business Development Agency, and small busi-
2 nesses, shall develop policy templates, toolkits, tip sheets,
3 configuration guidelines for commonly used hardware and
4 software, interactive tools, and other materials to assist
5 small businesses with complying with this section.

6 **SEC. 213. NOTIFICATION OF DATA BREACH OR DATA-SHAR-**
7 **ING ABUSE.**

8 (a) NOTIFICATION OF AGENCY.—

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

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

1 (b) NOTIFICATION OF OTHER COVERED ENTITY.—

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

20 (c) NOTIFICATION OF INDIVIDUALS.—

21 (1) IN GENERAL.—In the case of a data breach
22 or data-sharing abuse with respect to personal infor-
23 mation maintained by a covered entity (or a data
24 breach or data-sharing abuse about which a covered
25 entity is notified under subsection (b)), if such cov-

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

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

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

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

24 (d) RULE OF CONSTRUCTION.—This section shall not
25 apply to a covered entity if a person uses personal infor-

1 mation obtained from a data breach or data-sharing abuse
2 not involving such covered entity.

3 **TITLE III—DIGITAL PRIVACY**
4 **AGENCY**

5 **SEC. 301. ESTABLISHMENT; DIRECTOR AND DEPUTY DIREC-**
6 **TOR.**

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

11 (b) DIRECTOR.—

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

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

18 (3) QUALIFICATION.—The Director shall have a
19 professional background, experience, knowledge, and
20 expertise in the following:

21 (A) Privacy.

22 (B) Information security.

23 (C) Technology.

24 (D) Civil rights and civil liberties.

25 (4) TERM.—

1 (A) IN GENERAL.—The Director shall
2 serve for a term of 6 years.

3 (B) EXPIRATION OF TERM.—An individual
4 may serve as Director after the expiration of
5 the term for which appointed, until a successor
6 has been appointed and qualified.

7 (5) COMPENSATION.—

8 (A) IN GENERAL.—The Director shall be
9 compensated at the rate prescribed for level II
10 of the Executive Schedule under section 5313
11 of title 5, United States Code.

12 (B) CONFORMING AMENDMENT.—Section
13 5313 of title 5, United States Code, is amended
14 by inserting after the item relating to the
15 “Chief Executive Officer, United States Inter-
16 national Development Finance Corporation.”
17 the following new item: “Director of the Digital
18 Privacy Agency.”.

19 (c) DEPUTY DIRECTOR.—There is established the po-
20 sition of Deputy Director, who shall be appointed by the
21 Director.

22 (d) VACANCY OF OFFICE OF DIRECTOR.—

23 (1) IN GENERAL.—Sections 3345 through
24 3349d of title 5, United States Code (commonly
25 known as the “Federal Vacancies Reform Act of

1 1998’’), shall not apply to the office of the Director
2 of the Digital Privacy Agency.

3 (2) LINE OF SUCCESSION.—The Deputy Direc-
4 tor shall serve as acting Director if the Director
5 dies, resigns, or is otherwise unable to perform the
6 functions and duties of the office. The Director shall
7 establish a line of succession among senior officers
8 of the Digital Privacy Agency in the event the posi-
9 tion of Deputy Director is vacant to perform the
10 functions and duties of the Director temporarily in
11 an acting capacity.

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

16 (f) OFFICES.—The Director shall establish a prin-
17 cipal office and field offices of the Digital Privacy Agency
18 in locations that have high levels of activity by covered
19 entities, as determined by the Director.

20 **SEC. 302. AGENCY POWERS AND AUTHORITIES.**

21 (a) POWERS OF THE DIGITAL PRIVACY AGENCY.—
22 The Director is authorized to establish the general policies
23 of the Digital Privacy Agency with respect to all executive
24 and administrative functions, including—

1 (1) establishing of rules for conducting the gen-
2 eral business of the Digital Privacy Agency, in a
3 manner not inconsistent with this Act;

4 (2) binding the Digital Privacy Agency and en-
5 tering into contracts;

6 (3) directing the establishment and continued
7 operation of divisions or other offices within the Dig-
8 ital Privacy Agency, in order to carry out the re-
9 sponsibilities of the Digital Privacy Agency under
10 this Act, and to satisfy the requirements of other ap-
11 plicable law;

12 (4) coordinating and overseeing the operation of
13 all administrative, enforcement, and research activi-
14 ties of the Digital Privacy Agency;

15 (5) adopting and using a seal;

16 (6) determining the character of and the neces-
17 sity for the obligations and expenditures of the Dig-
18 ital Privacy Agency;

19 (7) appointing and supervising of personnel em-
20 ployed by the Digital Privacy Agency;

21 (8) distributing business among personnel ap-
22 pointed and supervised by the Director and among
23 administrative units of the Digital Privacy Agency;

24 (9) using and expending of funds;

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

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

6 (b) DELEGATION OF AUTHORITY.—The Director
7 may not delegate the power to appoint the Deputy Direc-
8 tor under section 301(c).

9 (c) AUTONOMY OF AGENCY REGARDING REC-
10 COMMENDATIONS AND TESTIMONY.—No officer or agency
11 of the United States may require the Director or any other
12 officer of the Digital Privacy Agency to submit legislative
13 recommendations, or testimony or comments on legisla-
14 tion, to any officer or agency of the United States for ap-
15 proval, comments, or review prior to the submission of
16 such recommendations, testimony, or comments to the
17 Congress, if such recommendations, testimony, or com-
18 ments to the Congress include a statement indicating that
19 the views expressed therein are those of the Director or
20 such officer, and do not necessarily reflect the views of
21 the President.

22 (d) RULEMAKING AUTHORITY.—

23 (1) IN GENERAL.—The Director may prescribe
24 such rules and regulations as may be necessary and
25 appropriate, and in the public interest, to imple-

1 ment, administer, and carry out this Act, and to
2 prevent evasions thereof.

3 (2) REGULATIONS.—The Digital Privacy Agen-
4 cy may issue regulations after notice and comment
5 in accordance with section 553 of title 5, United
6 States Code, as may be necessary to implement, ad-
7 minister, and carry out this Act.

8 (e) CONSULTATIONS.—In implementing or enforcing
9 this Act, the Director may consult with—

10 (1) Federal agencies that have—

11 (A) jurisdiction over Federal privacy laws;

12 and

13 (B) expertise in privacy or information se-
14 curity;

15 (2) State attorneys general, State privacy regu-
16 lators, and other State agencies that have expertise
17 in privacy or information security;

18 (3) international and intergovernmental bodies
19 that conduct activities relating to the privacy or in-
20 formation security;

21 (4) agencies of other countries that are similar
22 to the Digital Privacy Agency or have expertise in
23 privacy or information security;

24 (5) privacy and information security experts in
25 academia, government, civil society, or industry; and

1 (6) advisory boards of the Digital Privacy
2 Agency established under section 308, as appro-
3 priate.

4 (f) AGENCY DEFERENCE.—In any action for judicial
5 review of regulations or orders of the Digital Privacy
6 Agency, the reviewing court shall defer to the reasonable
7 interpretation by the Digital Privacy Agency of this Act.

8 **SEC. 303. REPORTING AND AUDIT REQUIREMENTS.**

9 (a) REPORTS REQUIRED.—

10 (1) IN GENERAL.—Not later than 6 months
11 after the date of the enactment of this Act, and
12 every 6 months thereafter, the Director shall submit
13 a report to the President and to the Committee on
14 Energy and Commerce, the Committee on the Judi-
15 ciary, and the Committee on Appropriations of the
16 House of Representatives and the Committee on
17 Commerce, Science, and Transportation, the Com-
18 mittee on the Judiciary, and the Committee on Ap-
19 propriations of the Senate, and shall publish such
20 report on the website of the Digital Privacy Agency.

21 (2) CONTENTS.—Each report required by sub-
22 section (a) shall include—

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

1 (B) a justification of the budget request of
2 the Digital Privacy Agency for the preceding
3 year, unless a justification for such year was in-
4 cluded in the preceding report submitted under
5 such subsection;

6 (C) a list of the significant rules and or-
7 ders adopted by the Digital Privacy Agency, as
8 well as other significant initiatives conducted by
9 the Digital Privacy Agency, during the pre-
10 ceding 6-month period and the plan of the Dig-
11 ital Privacy Agency for rules, orders, or other
12 initiatives to be undertaken during the upcom-
13 ing 6-month period;

14 (D) an analysis of complaints about the
15 privacy or security of personal information that
16 the Digital Privacy Agency has received and
17 collected in the database described in section
18 307(a) during the preceding 6-month period;

19 (E) a list, with a brief statement of the
20 issues, of the public enforcement actions to
21 which the Digital Privacy Agency was a party
22 during the preceding 6-month period; and

23 (F) an assessment of significant actions by
24 State attorneys general or State privacy regu-
25 lators relating to this Act or the rules pre-

1 scribed under this Act during the preceding 6-
2 month period.

3 (b) ANNUAL AUDITS.—The Director shall order an
4 annual independent audit of the operations and budget of
5 the Digital Privacy Agency.

6 **SEC. 304. RELATION TO OTHER AGENCIES.**

7 (a) COORDINATION.—

8 (1) IN GENERAL.—With respect to covered enti-
9 ties and service providers, to the extent that Federal
10 law authorizes the Digital Privacy Agency and an-
11 other Federal agency to enforce a Federal privacy
12 law, the head of the other Federal agency shall co-
13 ordinate with the Director of the Digital Privacy
14 Agency to promote consistent enforcement of this
15 Act and the other Federal privacy law.

16 (2) REFERRAL.—Any Federal agency author-
17 ized to enforce Federal privacy laws may recommend
18 in writing to the Digital Privacy Agency that the
19 Digital Privacy Agency initiate an enforcement pro-
20 ceeding, as the Digital Privacy Agency is authorized
21 by that Federal privacy law or by this Act.

22 (b) TRANSFERS FROM THE COMMISSION.—

23 (1) TRANSFERS OF AUTHORITY.—

24 (A) TRANSFER OF RULEMAKING AND CER-
25 TAIN OTHER AUTHORITIES UNDER FEDERAL

1 PRIVACY LAWS.—The Digital Privacy Agency
2 shall have all powers and duties under the Fed-
3 eral privacy laws to prescribe rules, issue guide-
4 lines, or to conduct studies or issue reports
5 mandated by such laws, that were vested in the
6 Commission on the effective date of this Act.
7 The authority of the Commission under Federal
8 privacy laws to prescribe rules, issue guidelines,
9 or conduct a study or issue a report mandated
10 under such law shall be transferred to the Dig-
11 ital Privacy Agency on the effective date of this
12 Act.

13 (B) TRANSFER OF ENFORCEMENT AU-
14 THORITY.—The Digital Privacy Agency may en-
15 force a rule prescribed by the Commission
16 under—

- 17 (i) Federal privacy laws; or
18 (ii) the Federal Trade Commission
19 Act (15 U.S.C. 41 et seq.) related to un-
20 fair or deceptive acts or practices relating
21 to privacy, information security, identity
22 theft, data abuses, and related matters.

23 (2) TRANSFER OF PRIVACY EMPLOYEES.—Any
24 employee of the Commission employed in a division,
25 bureau, office, or other subdivision of the Commis-

1 sion with the primary responsibility of admin-
2 istering, investigating, or enforcing Federal privacy
3 laws or applications of the Federal Trade Commis-
4 sion Act (15 U.S.C. 41 et seq.) related to unfair or
5 deceptive acts or practices relating to privacy, infor-
6 mation security, identity theft, data abuses, and re-
7 lated matters shall be transferred to the Digital Pri-
8 vacy Agency. Such employee shall be provided with
9 compensation and benefits not less than the equiva-
10 lent of compensation and benefits provided to such
11 employee on the date of enactment of this Act or
12 compensation and benefits provided to an employee
13 of the Digital Privacy Agency in comparable position
14 with comparable experience.

15 (c) PRESERVATION OF AUTHORITIES OF OTHER
16 AGENCIES.—Except as described in this section, no provi-
17 sion of this Act shall be construed as modifying, limiting,
18 or otherwise affecting the operation of any provision of
19 Federal law, or otherwise affecting the authority of any
20 Federal agency under a Federal privacy law or any other
21 law, including the ability of such Federal agency to pro-
22 mulgate regulations and enforce Federal privacy laws.

23 **SEC. 305. PERSONNEL.**

24 (a) PERSONNEL.—

1 (1) APPOINTMENT GENERALLY.—The Director
2 may fix the number of, and appoint and direct, all
3 employees of the Digital Privacy Agency, in accord-
4 ance with the applicable provisions of title 5, United
5 States Code. The Director may appoint personnel
6 without regard to the provisions of title 5, United
7 States Code, governing appointments in the competi-
8 tive service, so long as the Director sets require-
9 ments, conducts recruitment, and determines ap-
10 pointments in a fair, transparent, and equitable
11 manner.

12 (2) EMPLOYEES OF THE AGENCY.—The Direc-
13 tor is authorized to employ privacy experts, tech-
14 nologists, computer scientists, user experience de-
15 signers and researchers, data scientists, ethicists, at-
16 torneys, investigators, economists, civil rights ex-
17 perts, and other employees as the Director considers
18 necessary to conduct the business of the Digital Pri-
19 vacy Agency. Unless otherwise provided expressly by
20 law, any individual appointed under this section
21 shall be an employee, as defined in section 2105 of
22 title 5, United States Code, and subject to the provi-
23 sions of such title and other laws generally applica-
24 ble to the employees of an executive agency.

1 (3) EMPLOYEE COMPENSATION.—The Director
2 may fix and adjust the pay and benefits of personnel
3 as the Director considers desirable, competitive,
4 transparent, and equitable, without regard to the
5 provisions of chapter 51 and subchapter III of chap-
6 ter 53 of title 5, United States Code, relating to
7 classification and General Schedule pay rates, re-
8 spectively.

9 (4) LABOR-MANAGEMENT RELATIONS.—Chap-
10 ter 71 of title 5, United States Code, shall apply to
11 the Digital Privacy Agency and the employees of the
12 Digital Privacy Agency.

13 (b) ADDITIONAL ROLES.—

14 (1) CHIEF INFORMATION OFFICER.—

15 (A) DESIGNATION OF AN AGENCY CIO.—
16 Subchapter II of chapter 113 of subtitle III of
17 title 40, United States Code, is amended—

18 (i) in section 11315(c) by adding
19 “and of the Digital Privacy Agency” before
20 the em dash immediately preceding para-
21 graph (1); and

22 (ii) in section 11319(a)(1) by adding
23 “and the Digital Privacy Agency” before
24 the period.

1 (B) RESPONSIBILITY.—The Chief Informa-
2 tion Officer of the Digital Privacy Agency, as
3 designated by subparagraph (A), shall ensure
4 the Digital Privacy Agency uses technology effi-
5 ciency to implement, administer, and enforce
6 this Act and the rules and orders issued pursu-
7 ant to this Act.

8 (2) INSPECTOR GENERAL.—Section 401 of title
9 5, United States Code, is amended—

10 (A) in paragraph (1), by inserting “the
11 Digital Privacy Agency,” after “the Export-Im-
12 port Bank of the United States,”; and

13 (B) in paragraph (3), by inserting “the Di-
14 rector of the Digital Privacy Agency;” after
15 “the President of the Export-Import Bank of
16 the United States;”.

17 (3) OMBUD.—The Director shall appoint an
18 ombud who shall—

19 (A) act as a liaison between the Digital
20 Privacy Agency and any affected person with
21 respect to any problem that such person may
22 have in dealing with the Digital Privacy Agency
23 that results from the regulatory activities of the
24 Digital Privacy Agency; and

1 (B) ensure that safeguards exist to encour-
2 age complainants to come forward and preserve
3 confidentiality.

4 (c) **AUTHORITY TO ACCEPT FEDERAL DETAILEES.**—
5 The Director may accept officers or employees of the
6 United States or members of the Armed Forces on a detail
7 from an element of the Federal Government on a nonreim-
8 bursable basis, as jointly agreed to by the heads of the
9 receiving and detailing elements, for a period not to exceed
10 3 years.

11 **SEC. 306. OFFICE OF CIVIL RIGHTS.**

12 The Director shall establish an Office of Civil Rights
13 within the Digital Privacy Agency that shall have following
14 responsibilities:

15 (1) Providing oversight and enforcement of this
16 Act, rules and orders issued pursuant to this Act,
17 and Federal privacy laws to ensure that collecting,
18 processing, maintaining, and disclosing of personal
19 information is fair, equitable, and non-discrimina-
20 tory in treatment and effect, including through the
21 implementation and enforcement of section 207.

22 (2) Developing, establishing, and promoting
23 practices that affirmatively further equal oppor-
24 tunity to and expand access to employment (includ-
25 ing hiring, firing, promotion, demotion, and com-

1 pensation), credit and insurance (including denial of
2 an application or obtaining less favorable terms),
3 housing, education, professional certification, or the
4 provision of health care and related services.

5 (3) Coordinating the Digital Privacy Agency's
6 civil rights efforts with other Federal agencies and
7 State regulators, as appropriate, to promote con-
8 sistent, efficient, and effective enforcement of Fed-
9 eral civil rights laws.

10 (4) Working with civil rights advocates, privacy
11 experts, and other experts (including members of the
12 advisory boards established under section 308) on
13 the promotion of compliance with the civil rights
14 provisions under this Act, rules and orders issued
15 pursuant this Act, and Federal privacy laws.

16 (5) Liaising with communities and consumers
17 impacted by practices regulated by this Act and the
18 Digital Privacy Agency, to ensure that their needs
19 and views are appropriately taken into account.

20 (6) Providing annual reports to Congress on the
21 efforts of the Digital Privacy Agency to fulfill its
22 civil rights mandate.

23 (7) Such additional powers and duties as the
24 Director may determine are appropriate.

1 **SEC. 307. COMPLAINTS OF INDIVIDUALS.**

2 (a) IN GENERAL.—The Director shall establish a unit
3 within the Digital Privacy Agency the functions of which
4 shall include establishing a single, toll-free telephone num-
5 ber, a website, and a database or utilizing an existing
6 database to facilitate the centralized collection of, moni-
7 toring of, and response to complaints of individuals re-
8 garding the privacy or security of personal information.
9 The Director shall coordinate with other Federal agencies
10 with jurisdiction over Federal privacy laws to route com-
11 plaints to such agencies, where appropriate.

12 (b) ROUTING COMPLAINTS TO STATES.—To the ex-
13 tent practicable, State agencies (including State privacy
14 regulators) may receive appropriate complaints from the
15 systems established under subsection (a), if—

16 (1) the State agency system has the functional
17 capacity to receive calls or electronic reports routed
18 by the Digital Privacy Agency systems;

19 (2) the State agency has satisfied any condi-
20 tions of participation in the system that the Digital
21 Privacy Agency may establish, including treatment
22 of personal information and sharing of information
23 on complaint resolution or related compliance proce-
24 dures and resources; and

25 (3) participation by the State agency includes
26 measures necessary to provide for protection of per-

1 sonal information that conform to the standards for
2 protection of the confidentiality of personal informa-
3 tion and for data integrity and security that apply
4 to Federal agencies.

5 (c) DATA SHARING REQUIRED.—To facilitate inclu-
6 sion in the reports required by section 303 of the matters
7 regarding complaints of individuals required by subsection
8 (a)(2)(D) of such section to be included in such reports,
9 investigation and enforcement activities, and monitoring
10 of the privacy and security of personal information, the
11 Digital Privacy Agency shall share information about com-
12 plaints of individuals with Federal and State agencies (in-
13 cluding State privacy regulators) that have jurisdiction
14 over the privacy or security of personal information and
15 State attorneys general, subject to the standards applica-
16 ble to Federal agencies for the protection of the confiden-
17 tiality of personal information and for information secu-
18 rity and integrity. Other Federal agencies that have juris-
19 diction over the privacy or security of personal information
20 shall share data relating to complaints of individuals re-
21 garding the privacy or security of personal information
22 with the Digital Privacy Agency, subject to the standards
23 applicable to Federal agencies for the protection of con-
24 fidentiality of personal information and for information se-
25 curity and integrity.

1 (d) PUBLISHING OF COMPLAINTS.—

2 (1) CONSENT REQUIRED.—In collecting a com-
3 plaint from an individual, the Digital Privacy Agen-
4 cy shall request consent for publishing the complaint
5 without any information identifying the individual.

6 (2) PUBLIC DATABASE.—The Digital Privacy
7 Agency shall make publicly available on its website
8 a database of each complaint for which it has re-
9 ceived consent to publish the complaint from an in-
10 dividual who provided the complaint to the Digital
11 Privacy Agency.

12 (3) REDACTING INFORMATION.—When nec-
13 essary, the Digital Privacy Agency may redact infor-
14 mation from a published complaint to protect the
15 privacy of the individual.

16 **SEC. 308. ADVISORY BOARDS.**

17 (a) ESTABLISHMENT.—The Director shall establish
18 the following advisory boards to advise and consult with
19 the Digital Privacy Agency in the exercise of its functions
20 under this Act, and to provide information on emerging
21 practices relating to the treatment of personal information
22 by covered entities:

23 (1) The User Advisory Board, which shall be
24 composed of experts in consumer protection, privacy,
25 civil rights, and ethics.

1 (2) The Research Advisory Board, which shall
2 be composed of individuals with academic and re-
3 search expertise in privacy, cybersecurity, computer
4 science, innovation, design, ethics, economics, law,
5 and public policy.

6 (3) The Startup Advisory Board, which shall be
7 composed of representatives of small businesses and
8 investors in small businesses.

9 (4) The Product Advisory Board, which shall be
10 composed of technologists, computer scientists, de-
11 signers, product managers, attorneys, and other rep-
12 resentatives of covered entities.

13 (b) APPOINTMENTS.—The Director shall appoint
14 members to the advisory boards established under sub-
15 section (a) without regard to party affiliation.

16 (c) MEETINGS.—Each advisory board established
17 under subsection (a) shall meet from time to time at the
18 call of the Director, but, at a minimum, shall meet at least
19 twice in each calendar year.

20 (d) COMPENSATION AND TRAVEL EXPENSES.—Mem-
21 bers of the advisory boards established under subsection
22 (a) who are not full-time employees of the United States
23 shall—

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

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

8 **SEC. 309. AUTHORIZATION OF APPROPRIATIONS.**

9 There are authorized to be appropriated to the Direc-
 10 tor to carry out this Act \$550,000,000 for each of the
 11 fiscal years 2026, 2027, 2028, 2029, and 2030.

12 **TITLE IV—ENFORCEMENT**

13 **SEC. 401. INVESTIGATIONS AND ADMINISTRATIVE DIS-**
 14 **COVERY.**

15 (a) **JOINT INVESTIGATIONS.**—The Digital Privacy
 16 Agency or, where appropriate, a Digital Privacy Agency
 17 investigator, may conduct investigations and make re-
 18 quests for information, as authorized under this Act, on
 19 a joint basis with another Federal agency, a State attor-
 20 ney general, or a State privacy regulator.

21 (b) **SUBPOENAS.**—

22 (1) **IN GENERAL.**—The Digital Privacy Agency
 23 or a Digital Privacy Agency investigator may issue
 24 subpoenas for the attendance and testimony of wit-
 25 nesses and the production of relevant papers, books,

1 documents, or other material in connection with
2 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 Digital Privacy
9 Agency or a Digital Privacy Agency investigator and
10 after notice to such person, may issue an order re-
11 quiring such person to appear and give testimony or
12 to appear and produce documents 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 Digital Pri-
18 vacy Agency has reason to believe that any person
19 may be in possession, custody, or control of any doc-
20 umentary material or tangible things, or may have
21 any information, relevant to a violation, the Digital
22 Privacy Agency may, before the institution of any
23 proceedings under this Act, issue in writing, and
24 cause to be served upon such person, a civil inves-
25 tigative demand requiring such person to—

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

5 (B) submit such tangible things;

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

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

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

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

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

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

1 (B) prescribe a return date or dates which
2 will provide a reasonable period of time within
3 which the material so demanded may be assem-
4 bled and made available for inspection and
5 copying or reproduction; and

6 (C) identify the custodian to whom such
7 material shall be made available.

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

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

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

19 (C) identify the custodian to whom such
20 things shall be submitted.

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

1 (A) propound with definiteness and cer-
2 tainty the reports to be produced or the ques-
3 tions to be answered;

4 (B) prescribe a date or dates at which time
5 written reports or answers to questions shall be
6 submitted; and

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

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

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

13 (B) identify a Digital Privacy Agency in-
14 vestigator who shall conduct the investigation
15 and the custodian to whom the transcript of
16 such investigation shall be submitted.

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

20 (A) by any Digital Privacy Agency investi-
21 gator at any place within the territorial juris-
22 diction of any court of the United States; and

23 (B) upon any person who is not found
24 within the territorial jurisdiction of any court of
25 the United States—

1 (i) in such manner as the Federal
2 Rules of Civil Procedure prescribe for serv-
3 ice in a foreign nation; and

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

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

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

1 (B) delivering a duly executed copy of such
2 demand or petition to the principal office or
3 place of business of the person to be served; or

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

9 (9) PROOF OF SERVICE.—

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

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

20 (10) PRODUCTION OF DOCUMENTARY MATE-
21 RIAL.—The production of documentary material in
22 response to a civil investigative demand shall be
23 made under a sworn certificate, in such form as the
24 demand designates, by the person, if a natural per-
25 son, to whom the demand is directed or, if not a

1 natural person, by any person having knowledge of
2 the facts and circumstances relating to such produc-
3 tion, to the effect that all of the documentary mate-
4 rial required by the demand and in the possession,
5 custody, or control of the person to whom the de-
6 mand is directed has been produced and made avail-
7 able to the custodian.

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

20 (12) SEPARATE ANSWERS.—Each reporting re-
21 quirement or question in a civil investigative demand
22 shall be answered separately and fully in writing
23 under oath, unless it is objected to, in which event
24 the reasons for the objection shall be stated in lieu
25 of an answer, and it shall be submitted under a

1 sworn certificate, in such form as the demand des-
2 ignates, by the person, if a natural person, to whom
3 the demand is directed or, if not a natural person,
4 by any person responsible for answering each report-
5 ing requirement or question, to the effect that all in-
6 formation required by the demand and in the posses-
7 sion, custody, control, or knowledge of the person to
8 whom the demand is directed has been submitted.

9 (13) TESTIMONY.—

10 (A) IN GENERAL.—

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

1 (ii) TRANSCRIPTION.—The testimony
2 shall be taken stenographically and tran-
3 scribed.

4 (B) PARTIES PRESENT.—Any Digital Pri-
5 vacy Agency investigator before whom oral tes-
6 timony is to be taken shall exclude from the
7 place where the testimony is to be taken all
8 other persons, except the person giving the tes-
9 timony, the attorney for that person, the officer
10 before whom the testimony is to be taken, an
11 investigator or representative of an agency with
12 which the Digital Privacy Agency is engaged in
13 a joint investigation, and any stenographer tak-
14 ing such testimony.

15 (C) LOCATION.—The oral testimony of any
16 person taken pursuant to a civil investigative
17 demand shall be taken in the judicial district of
18 the United States in which such person resides,
19 is found, or transacts business, or in such other
20 place as may be agreed upon by the Digital Pri-
21 vacy Agency investigator before whom the oral
22 testimony of such person is to be taken and
23 such person.

24 (D) ATTORNEY REPRESENTATION.—

1 (i) IN GENERAL.—Any person com-
2 pelled to appear under a civil investigative
3 demand for oral testimony pursuant to this
4 subsection may be accompanied, rep-
5 resented, and advised by an attorney.

6 (ii) AUTHORITY.—The attorney may
7 advise a person described in clause (i), in
8 confidence, either upon the request of such
9 person or upon the initiative of the attor-
10 ney, with respect to any question asked of
11 such person.

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

1 and such person or attorney shall not oth-
2 erwise interrupt the oral examination.

3 (iv) REFUSAL TO ANSWER.—If a per-
4 son described in clause (i) refuses to an-
5 swer any question—

6 (I) the Digital Privacy Agency
7 may petition the district court of the
8 United States pursuant to this section
9 for an order compelling such person
10 to answer such question; and

11 (II) if the refusal is on grounds
12 of the privilege against self-incrimina-
13 tion, the testimony of such person
14 may be compelled in accordance with
15 the provisions of section 6004 of title
16 18, United States Code.

17 (E) TRANSCRIPTS.—For purposes of this
18 subsection—

19 (i) after the testimony of any witness
20 is fully transcribed, the Digital Privacy
21 Agency investigator shall afford the wit-
22 ness (who may be accompanied by an at-
23 torney) a reasonable opportunity to exam-
24 ine the transcript;

1 (ii) the transcript shall be read to or
2 by the witness, unless such examination
3 and reading are waived by the witness;

4 (iii) any changes in form or substance
5 which the witness desires to make shall be
6 entered and identified upon the transcript
7 by the Digital Privacy Agency investigator,
8 with a statement of the reasons given by
9 the witness for making such changes;

10 (iv) the transcript shall be signed by
11 the witness, unless the witness in writing
12 waives the signing, is ill, cannot be found,
13 or refuses to sign; and

14 (v) if the transcript is not signed by
15 the witness during the 30-day period fol-
16 lowing the date on which the witness is
17 first afforded a reasonable opportunity to
18 examine the transcript, the Digital Privacy
19 Agency investigator shall sign the tran-
20 script and state on the record the fact of
21 the waiver, illness, absence of the witness,
22 or the refusal to sign, together with any
23 reasons given for the failure to sign.

24 (F) CERTIFICATION BY INVESTIGATOR.—

25 The Digital Privacy Agency investigator shall

1 certify on the transcript that the witness was
2 duly sworn by such Digital Privacy Agency in-
3 vestigator and that the transcript is a true
4 record of the testimony given by the witness,
5 and the Digital Privacy Agency investigator
6 shall promptly deliver the transcript or send it
7 by registered or certified mail to the custodian.

8 (G) COPY OF TRANSCRIPT.—The Digital
9 Privacy Agency investigator shall furnish a copy
10 of the transcript (upon payment of reasonable
11 charges for the transcript) to the witness only,
12 except that the Digital Privacy Agency may for
13 good cause limit such witness to inspection of
14 the official transcript of the testimony of such
15 witness.

16 (H) WITNESS FEES.—Any witness appear-
17 ing for the taking of oral testimony pursuant to
18 a civil investigative demand shall be entitled to
19 the same fees and mileage which are paid to
20 witnesses in the district courts of the United
21 States.

22 (d) CONFIDENTIAL TREATMENT OF DEMAND MATE-
23 RIAL.—

24 (1) IN GENERAL.—Documentary materials and
25 tangible things received as a result of a civil inves-

1 tigtative demand shall be subject to requirements and
2 procedures regarding confidentiality, in accordance
3 with rules established by the Digital Privacy Agency.

4 (2) DISCLOSURE TO CONGRESS.—No rule es-
5 tablished by the Digital Privacy Agency regarding
6 the confidentiality of materials submitted to, or oth-
7 erwise obtained by, the Digital Privacy Agency shall
8 be intended to prevent disclosure to either House of
9 Congress or to an appropriate committee of the Con-
10 congress, except that the Digital Privacy Agency is per-
11 mitted to adopt rules allowing prior notice to any
12 party that owns or otherwise provided the material
13 to the Digital Privacy Agency and had designated
14 such material as confidential.

15 (e) PETITION FOR ENFORCEMENT.—

16 (1) IN GENERAL.—Whenever any person fails
17 to comply with any civil investigative demand duly
18 served upon such person under this section, or when-
19 ever satisfactory copying or reproduction of material
20 requested pursuant to the demand cannot be accom-
21 plished and such person refuses to surrender such
22 material, the Digital Privacy Agency, through such
23 officers or attorneys as it may designate, may file,
24 in the district court of the United States for any ju-
25 dicial district in which such person resides, is found,

1 or transacts business, and serve upon such person,
2 a petition for an order of such court for the enforce-
3 ment of this section.

4 (2) SERVICE OF PROCESS.—All process of any
5 court to which application may be made as provided
6 in this subsection may be served in any judicial dis-
7 trict.

8 (f) PETITION FOR ORDER MODIFYING OR SETTING
9 ASIDE DEMAND.—

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

22 (2) COMPLIANCE DURING PENDENCY.—The
23 time permitted for compliance with the demand in
24 whole or in part, as determined proper and ordered
25 by the Digital Privacy Agency, shall not run during

1 the pendency of a petition under paragraph (1) at
2 the Digital Privacy Agency, except that such person
3 shall comply with any portions of the demand not
4 sought to be modified or set aside.

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

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

24 (h) JURISDICTION OF COURT.—

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

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

11 **SEC. 402. HEARINGS AND ADJUDICATION PROCEEDINGS.**

12 (a) IN GENERAL.—Except as provided in subsection
13 (b), the Digital Privacy Agency is authorized to conduct
14 hearings and adjudication proceedings with respect to any
15 person in the manner prescribed by subchapter II of chap-
16 ter 5 of title 5, United States Code, in order to ensure
17 or enforce compliance with this Act and the rules pre-
18 scribed under this Act.

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

21 (1) ORDERS AUTHORIZED.—

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

1 scribed under this Act, the Digital Privacy
2 Agency may issue and serve upon the person a
3 notice of charges in respect thereof.

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

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

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

1 ital Privacy Agency may issue an order to cease
2 and desist from the violation. Such order may,
3 by provisions which may be mandatory or other-
4 wise, require the person to cease and desist
5 from the subject act or omission, and to take
6 affirmative action to correct the conditions re-
7 sulting from any such violation.

8 (2) EFFECTIVENESS OF ORDER.—A cease-and-
9 desist order shall become effective at the expiration
10 of 30 days after the date of service of the order
11 under paragraph (1)(D) (except in the case of a
12 cease-and-desist order issued upon consent, which
13 shall become effective 180 days after the date of
14 service of the notice of charges under paragraph
15 (1)(A)), and shall remain effective and enforceable
16 as provided therein, except to such extent as the
17 order is stayed, modified, terminated, or set aside by
18 action of the Digital Privacy Agency or a reviewing
19 court.

20 (3) DECISION AND APPEAL.—Any hearing pro-
21 vided for in this subsection shall be held in the Fed-
22 eral judicial district or in the territory in which the
23 residence or principal office or place of business of
24 the person is located unless the person consents to
25 another place, and shall be conducted in accordance

1 with the provisions of subchapter II of chapter 5 of
2 title 5, United States Code. After such hearing, and
3 not later than 90 days after the Digital Privacy
4 Agency has served the notice under paragraph
5 (1)(A), the Digital Privacy Agency shall render its
6 decision (which shall include findings of fact upon
7 which its decision is predicated) and shall issue and
8 serve upon each such party an order or orders con-
9 sistent with the provisions of this section. Judicial
10 review of any such order shall be exclusively as pro-
11 vided in this subsection. Unless a petition for review
12 is timely filed in a court of appeals of the United
13 States, as provided in paragraph (4), and thereafter
14 until the record in the proceeding has been filed as
15 provided in paragraph (4), the Digital Privacy Agen-
16 cy may at any time, upon such notice and in such
17 manner as the Digital Privacy Agency shall deter-
18 mine proper, modify, terminate, or set aside any
19 such order. Upon filing of the record as provided,
20 the Digital Privacy Agency may modify, terminate,
21 or set aside any such order with permission of the
22 court.

23 (4) APPEAL TO COURT OF APPEALS.—Any
24 party to any proceeding under this subsection may
25 obtain a review of any order served pursuant to this

1 subsection (other than an order issued with the con-
2 sent of the party) by filing in the court of appeals
3 of the United States for the circuit in which the resi-
4 dence or principal office or place of business of the
5 party is located, or in the United States Court of
6 Appeals for the District of Columbia Circuit, within
7 30 days after the date of service of such order, a
8 written petition praying that the order of the Digital
9 Privacy Agency be modified, terminated, or set
10 aside. A copy of such petition shall be forthwith
11 transmitted by the clerk of the court to the Digital
12 Privacy Agency, and thereupon the Digital Privacy
13 Agency shall file in the court the record in the pro-
14 ceeding, as provided in section 2112 of title 28,
15 United States Code. Upon the filing of such petition,
16 such court shall have jurisdiction, which upon the
17 filing of the record shall be exclusive, to affirm,
18 modify, terminate, or set aside, in whole or in part,
19 the order of the Digital Privacy Agency. Review of
20 such proceedings shall be had as provided in chapter
21 7 of title 5, United States Code.

22 (5) NO STAY.—The commencement of pro-
23 ceedings for judicial review under paragraph (4)
24 shall not, unless specifically ordered by the court,

1 operate as a stay of any order issued by the Digital
2 Privacy Agency.

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

5 (1) IN GENERAL.—Whenever the Digital Pri-
6 vacy Agency determines that the violation specified
7 in the notice of charges served upon a person pursu-
8 ant to subsection (b), or the continuation thereof, is
9 likely to cause the person to be insolvent or other-
10 wise prejudice the interests of individuals before the
11 completion of the proceedings conducted pursuant to
12 subsection (b), the Digital Privacy Agency may issue
13 a temporary order requiring the person to cease and
14 desist from any such violation and to take affirma-
15 tive action to prevent or remedy such insolvency or
16 other condition pending completion of such pro-
17 ceedings. Such order may include any requirement
18 authorized under this title. Such order shall become
19 effective upon service upon the person and, unless
20 set aside, limited, or suspended by a court in pro-
21 ceedings authorized by paragraph (2), shall remain
22 effective and enforceable pending the completion of
23 the administrative proceedings pursuant to such no-
24 tice and until such time as the Digital Privacy Agen-
25 cy shall dismiss the charges specified in such notice,

1 or if a cease-and-desist order is issued against the
2 person, until the effective date of such order.

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

16 (d) SPECIAL RULES FOR ENFORCEMENT OF OR-
17 DERS.—The Digital Privacy Agency may in its discretion
18 apply to the United States district court within the juris-
19 diction of which the residence or principal office or place
20 of business of a person is located, for the enforcement of
21 any effective and outstanding order issued under this sec-
22 tion against such person, and such court shall have juris-
23 diction and power to order and require compliance with
24 such order.

1 **SEC. 403. LITIGATION AUTHORITY.**

2 (a) IN GENERAL.—If a person violates any provision
3 of this Act or a rule or order prescribed under this Act,
4 the Digital Privacy Agency may commence a civil action
5 against such person in a court of competent jurisdiction
6 to impose a civil penalty or to seek all appropriate legal
7 and equitable relief, including a permanent or temporary
8 injunction.

9 (b) COMPROMISE OF ACTIONS.—The Digital Privacy
10 Agency may compromise or settle any action, suit, or other
11 court proceeding to which the Digital Privacy Agency is
12 a party if such compromise is approved by the court.

13 (c) NOTICE TO THE ATTORNEY GENERAL OF THE
14 UNITED STATES.—

15 (1) IN GENERAL.—When commencing a civil
16 action under this Act or regulations or rules or or-
17 ders issued pursuant to this Act, the Digital Privacy
18 Agency shall notify the Attorney General.

19 (2) NOTICE AND COORDINATION.—

20 (A) NOTICE OF OTHER ACTIONS.—In addi-
21 tion to any notice required under paragraph
22 (1), the Digital Privacy Agency shall notify the
23 Attorney General concerning any action, suit,
24 or other court proceeding to which the Digital
25 Privacy Agency is a party.

1 (B) COORDINATION.—In order to avoid
2 conflicts and promote consistency regarding liti-
3 gation of matters under Federal law, the Attor-
4 ney General and the Digital Privacy Agency
5 shall consult regarding the coordination of in-
6 vestigations and proceedings, including by nego-
7 tiating an agreement for coordination not later
8 than 180 days after the effective date of this
9 Act. The agreement under this subparagraph
10 shall include provisions to ensure that parallel
11 investigations and proceedings involving this
12 Act and the rules prescribed under this Act are
13 conducted in a manner that avoids conflicts and
14 does not impede the ability of the Attorney
15 General to prosecute violations of Federal
16 criminal laws.

17 (C) RULE OF CONSTRUCTION.—Nothing in
18 this paragraph shall be construed to limit the
19 authority of the Digital Privacy Agency under
20 this Act, including the authority to interpret
21 this Act.

22 (d) APPEARANCE BEFORE THE SUPREME COURT.—

23 The Digital Privacy Agency may represent itself in its own
24 name before the Supreme Court of the United States, if
25 the Digital Privacy Agency makes a written request to the

1 Attorney General within the 10-day period which begins
2 on the date of entry of the judgment which would permit
3 any party to file a petition for writ of certiorari, and the
4 Attorney General concurs with such request or fails to
5 take action within 60 days of the request of the Digital
6 Privacy Agency.

7 (e) FORUM.—Any civil action brought under this Act
8 or regulations or rules or orders issued pursuant to this
9 Act may be brought in an appropriate district court of
10 the United States or an appropriate State court.

11 (f) TIME FOR BRINGING ACTION.—Except as other-
12 wise permitted by law or equity, no action may be brought
13 under this Act more than 3 years after the date of dis-
14 covery of the violation to which the action relates.

15 **SEC. 404. ENFORCEMENT BY STATES.**

16 (a) CIVIL ACTION.—In any case in which a State at-
17 torney general or a State privacy regulator has reason to
18 believe that an interest of the residents of a State has been
19 or is adversely affected by any person who violates any
20 provision of this Act or a rule or order prescribed under
21 this Act, the State attorney general or State privacy regu-
22 lator, as *parens patriae*, may bring a civil action on behalf
23 of the residents of the State in an appropriate State court
24 or an appropriate district court of the United States to—

1 (1) enjoin further violation of such provision by
2 the defendant;

3 (2) compel compliance with such provision; or

4 (3) obtain relief under section 406.

5 (b) RIGHTS OF AGENCY.—Before initiating a civil ac-
6 tion under subsection (a), the State attorney general or
7 State privacy regulator, as the case may be, shall notify
8 the Digital Privacy Agency in writing of such civil action.
9 Upon receiving notice with respect to a civil action, the
10 Digital Privacy Agency may—

11 (1) intervene in such action; and

12 (2) upon intervening—

13 (A) be heard on all matters arising in such
14 civil action; and

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

17 (c) PREEMPTIVE ACTION BY AGENCY.—If the Digital
18 Privacy Agency institutes a civil action for violation of any
19 provision of this Act or a rule or order prescribed under
20 this Act, no State attorney general or State privacy regu-
21 lator may bring a civil action against any defendant
22 named in the complaint of the Digital Privacy Agency for
23 a violation of such provision that is alleged in such com-
24 plaint.

1 **SEC. 405. PRIVATE RIGHTS OF ACTION.**

2 (a) INJUNCTIVE RELIEF.—A person who is aggrieved
3 by a violation of this Act may bring a civil action for de-
4 claratory or injunctive relief in any court of competent ju-
5 risdiction.

6 (b) CIVIL ACTION FOR DAMAGES.—Except for claims
7 under rule 23 of the Federal Rules of Civil Procedure or
8 a similar judicial procedure authorizing an action to be
9 brought by 1 or more representatives, a person who is ag-
10 grieved by a violation of this Act may bring a civil action
11 for damages in any court of competent jurisdiction.

12 (c) NONPROFIT COLLECTIVE REPRESENTATION.—
13 An individual shall have the right to appoint a nonprofit
14 organization (as described in section 501(c)(3) of the In-
15 ternal Revenue Code of 1986 and exempt from taxation
16 under section 501(a) of such Code) which has been prop-
17 erly constituted in accordance with the law, has statutory
18 objectives which are in the public interest, and is active
19 in the field of the protection of individual rights and free-
20 doms with regard to the protection of privacy and informa-
21 tion security to lodge the complaint on behalf of such indi-
22 vidual to exercise the rights referred to in this Act on be-
23 half of such individual.

24 (1) A nonprofit may represent a class of ag-
25 grieved individuals.

1 (2) A prevailing nonprofit shall receive reason-
2 able compensation for expenses, including attorneys'
3 fees.

4 (3) Individuals shall receive an equally divided
5 share of the total damages.

6 (d) STATE APPOINTMENT.—A State may provide
7 that any body, organization, or association referred to in
8 subsection (c), independent of an individual's appoint-
9 ment, has the right to lodge, in that State, a complaint
10 with the Digital Privacy Agency and to exercise the rights
11 referred to in this Act if it considers that the rights of
12 an individual under this Act have been infringed.

13 **SEC. 406. RELIEF AVAILABLE.**

14 (a) CIVIL ACTIONS AND ADJUDICATION PRO-
15 CEEDINGS.—

16 (1) JURISDICTION.—In any civil action or any
17 adjudication proceeding brought by the Digital Pri-
18 vacy Agency, a State attorney general, or State pri-
19 vacy regulator under any provision of this Act or a
20 rule or order prescribed under this Act, the court or
21 the Digital Privacy Agency (as the case may be)
22 shall have jurisdiction to grant any appropriate legal
23 or equitable relief with respect to a violation of such
24 provision.

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

3 (A) rescission or reformation of contracts;

4 (B) refund of moneys;

5 (C) restitution;

6 (D) disgorgement or compensation for un-
7 just enrichment;

8 (E) payment of damages or other mone-
9 tary relief;

10 (F) public notification regarding the viola-
11 tion, including the costs of notification;

12 (G) limits on the activities or functions of
13 the person; and

14 (H) civil money penalties, as provided in
15 subsection (c).

16 (3) NO EXEMPLARY OR PUNITIVE DAMAGES.—

17 Nothing in this subsection shall be construed as au-
18 thorizing the imposition of exemplary or punitive
19 damages.

20 (b) RECOVERY OF COSTS.—In any civil action
21 brought by the Digital Privacy Agency, State attorney
22 general, or State privacy regulator under any provision of
23 this Act or a rule or order prescribed under this Act, the
24 Digital Privacy Agency, State attorney general, or State
25 privacy regulator may recover its costs in connection with

1 prosecuting such action if the Digital Privacy Agency or
2 State attorney general is the prevailing party in the action.

3 (c) CIVIL MONEY PENALTY IN COURT AND ADMINIS-
4 TRATIVE ACTIONS.—

5 (1) IN GENERAL.—Any person who violates,
6 through any act or omission, any provision of this
7 Act or a rule or order issued pursuant to this Act
8 shall forfeit and pay a civil penalty under this sub-
9 section.

10 (2) PENALTY AMOUNT.—

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

14 (i) the maximum civil penalty for
15 which a person, partnership, or corporation
16 may be liable under section 5(m)(1)(A) of
17 the Federal Trade Commission Act (15
18 U.S.C. 45(m)(1)(A)) for a violation of a
19 rule under such Act respecting unfair or
20 deceptive acts or practices, as adjusted
21 under the Federal Civil Penalties Inflation
22 Adjustment Act of 1990 (28 U.S.C. 2461
23 note); and

1 (ii) the number of individuals whose
2 personal information is affected by the vio-
3 lation.

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

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

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

18 (B) the gravity of the violation;

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

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

25 (E) the history of previous violations; and

1 (F) such other matters as justice may re-
2 quire.

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

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

18 (A) the Digital Privacy Agency, State at-
19 torney general, or State privacy regulator gives
20 notice and an opportunity for a hearing to the
21 person accused of the violation; or

22 (B) the appropriate court has ordered such
23 assessment and entered judgment in favor of
24 the Digital Privacy Agency, State attorney gen-
25 eral, or State privacy regulator.

1 **SEC. 407. REFERRAL FOR CRIMINAL PROCEEDINGS.**

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

10 **SEC. 408. WHISTLEBLOWER ENFORCEMENT.**

11 (a) IN GENERAL.—Any person who becomes aware,
12 based on nonpublic information, that a covered entity has
13 violated this Act may file a civil action for civil penalties,
14 if prior to filing such action, the person files with the Di-
15 rector a written request for the Director to commence the
16 action. The request shall include a clear and concise state-
17 ment of the grounds for believing a cause of action exists.
18 The person shall make the nonpublic information available
19 to the Director upon request:

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

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

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

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

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

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

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

1 the proceeds of the action and shall be paid out of
2 the proceeds.

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

5 **SEC. 501. EFFECTIVE DATE.**

6 (a) IN GENERAL.—This Act shall apply beginning on
7 the date that is 1 year after the date of the enactment
8 of this Act.

9 (b) AUTHORITY TO PROMULGATE REGULATIONS AND
10 TAKE CERTAIN OTHER ACTIONS.—Nothing in subsection
11 (a) affects the authority of the Digital Privacy Agency to
12 take an action expressly required by a provision of this
13 Act to be taken before the effective date described in such
14 subsection.

15 **SEC. 502. RELATION TO OTHER FEDERAL LAW.**

16 Nothing in this Act shall be construed to modify,
17 limit, or supersede the operation of any privacy or security
18 provision in the following:

19 (1) Section 552a of title 5, United States Code
20 (commonly known as the “Privacy Act of 1974”).

21 (2) The Right to Financial Privacy Act of 1978
22 (12 U.S.C. 3401 et seq.).

23 (3) The Fair Credit Reporting Act (15 U.S.C.
24 1681 et seq.).

1 (4) The Fair Debt Collection Practices Act (15
2 U.S.C. 1692 et seq.).

3 (5) The Children’s Online Privacy Protection
4 Act of 1998 (15 U.S.C. 6501 et seq.).

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

7 (7) Chapter 119, 123, or 206 of title 18,
8 United States Code.

9 (8) Section 444 of the General Education Pro-
10 visions Act (20 U.S.C. 1232g) (commonly known as
11 the “Family Educational Rights and Privacy Act of
12 1974”).

13 (9) Section 445 of the General Education Pro-
14 visions Act (20 U.S.C. 1232h).

15 (10) The Privacy Protection Act of 1980 (42
16 U.S.C. 2000aa et seq.).

17 (11) The regulations promulgated under section
18 264(c) of the Health Insurance Portability and Ac-
19 countability Act of 1996 (42 U.S.C. 1320d–2 note),
20 as those regulations relate to—

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

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

4 (12) The Communications Assistance for Law
5 Enforcement Act (47 U.S.C. 1001 et seq.).

6 (13) Section 222, 227, 338, or 631 of the Com-
7 munications Act of 1934 (47 U.S.C. 222, 227, 338,
8 or 551).

9 (14) The E-Government Act of 2002 (44
10 U.S.C. 101 et seq.).

11 (15) The Paperwork Reduction Act of 1995 (44
12 U.S.C. 3501 et seq.).

13 (16) The Federal Information Security Manage-
14 ment Act of 2002 (44 U.S.C. 3541 et seq.).

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

23 (18) The National Security Act of 1947 (50
24 U.S.C. 3001 et seq.).

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

3 (20) The Civil Rights Act of 1964 (Public Law
4 88–352, 78 Stat. 241).

5 (21) The Americans with Disabilities Act (42
6 U.S.C. 12101 et seq.).

7 (22) The Fair Housing Act (42 U.S.C. 3601 et
8 seq.).

9 (23) The Consumer Financial Protection Act of
10 2010 (12 U.S.C. 5481 et seq.).

11 (24) The Equal Credit Opportunity Act (15
12 U.S.C. 1691 et seq.).

13 (25) The Age Discrimination in Employment
14 Act (29 U.S.C. 621 et seq.).

15 (26) The Genetic Information Nondiscrimina-
16 tion Act (Public Law 110–233, 122 Stat. 881).

17 (27) Subpart A of part 46 of title 45, Code of
18 Federal Regulations (commonly known as the “Com-
19 mon Rule”).

20 (28) The Driver’s Privacy Protection Act of
21 1994 (18 U.S.C. 2721 et seq.).

22 (29) The Video Privacy Protection Act (18
23 U.S.C. 2710 et seq.).

24 (30) Chapters 61, 68, 75, and 76 of the Inter-
25 nal Revenue Code of 1986.

1 (31) Section 1106 of the Social Security Act
2 (42 U.S.C. 1306).

3 (32) The Stored Communications Act (18
4 U.S.C. 2701 et seq.).

5 (33) Any other privacy or information security
6 provision of Federal law.

7 **SEC. 503. RELATION TO STATE LAW.**

8 This Act, and any amendment, standard, rule, re-
9 quirement, assessment, or regulation promulgated under
10 this Act, does not annul, alter, affect, or exempt any per-
11 son subject to the provisions of this Act from complying
12 with the laws of any State or political subdivision of a
13 State with respect to privacy or consumer protection, ex-
14 cept to the extent that those laws are inconsistent with
15 any provisions of this Act, and then only to the extent
16 of the inconsistency. For purposes of this section, a law
17 of a State or political subdivision of a State is not incon-
18 sistent with this Act if the protection such law affords any
19 consumer is greater than the protection provided by this
20 Act.

21 **SEC. 504. SEVERABILITY.**

22 If any provision of this Act or the amendments made
23 by this Act, or the application thereof, is held unconstitu-
24 tional or otherwise invalid, the validity of the remainder

1 of the Act, the amendments, and the application of such
2 provision shall not be affected thereby.

3 **TITLE VI—NIST AND NSF** 4 **ACTIVITIES**

5 **SEC. 601. NATIONAL INSTITUTE OF STANDARDS AND TECH-**
6 **NOLOGY PRIVACY RESEARCH AND DEVELOP-**
7 **MENT.**

8 Section 2 of the National Institute of Standards and
9 Technology Act (15 U.S.C. 272) is amended by adding
10 at the end the following:

11 “(f) PRIVACY RISK MANAGEMENT RESEARCH.—In
12 carrying out the activities under subsection (c)(19), the
13 Director, in consultation and collaboration with the Direc-
14 tor of the Digital Privacy Agency, shall, to the extent prac-
15 ticable and appropriate carry out the following:

16 “(1) Develop, and periodically update, in col-
17 laboration with appropriate Federal agencies, indus-
18 try, State, local, and Tribal governments, civil soci-
19 ety, other nonprofit organizations, and the Informa-
20 tion Security and Privacy Advisory Board, a privacy
21 risk management framework that covers risks associ-
22 ated with data processing and that—

23 “(A) identifies voluntary, consensus-based
24 technical standards, guidelines, best practices,
25 methodologies, procedures, and processes for—

1 “(i) developing privacy-enhanced in-
2 formation systems and networks, including
3 emerging technologies; and

4 “(ii) assessing and mitigating privacy
5 risks to help organizations protect individ-
6 uals’ privacy in information systems and
7 networks;

8 “(B) establishes common definitions and
9 characterizations for aspects of privacy risk
10 management;

11 “(C) provides case studies and risk profiles
12 of framework implementation;

13 “(D) provides guidance to enable organiza-
14 tions to use the framework to meet privacy re-
15 quirements from Federal, State, local, and
16 Tribal governments and international policy-
17 makers;

18 “(E) incorporates voluntary, consensus-
19 based technical standards and best practices;

20 “(F) facilitates use by regulators and mar-
21 kets with the aim of reducing barriers to trade;
22 and

23 “(G) does not prescribe or otherwise re-
24 quire the use of specific information or commu-
25 nications technology products or services.

1 “(2) Carry out research associated with miti-
2 gating privacy risks associated with information sys-
3 tems and networks, including to inform periodic up-
4 dates to the privacy risk management framework de-
5 veloped pursuant to paragraph (1).

6 “(3) In consultation with the Director of the
7 Digital Privacy Agency, the Federal Trade Commis-
8 sion, and other related sector-specific risk manage-
9 ment agencies, support the development of guidance
10 and risk profiles to help organizations utilize the pri-
11 vacy risk management framework developed pursu-
12 ant to paragraph (1), to the extent practicable, to
13 adopt privacy requirements and regulations estab-
14 lished by the Federal Government, States, and inter-
15 national policymakers.

16 “(4) Support activities to improve the efficacy
17 and applicability of privacy-preserving computing,
18 de-identification techniques and processes, and other
19 technological means of mitigating individuals’ pri-
20 vacy risks by enhancing predictability, manage-
21 ability, disassociability, and confidentiality.

22 “(5) Support and strategically engage in the de-
23 velopment of voluntary, consensus-based technical
24 standards for privacy-enhanced systems and net-
25 works, including international technical standards,

1 through open, transparent, and consensus-based
2 processes.

3 “(6) Conduct such other activities as deter-
4 mined necessary by the Director to help public and
5 private sector organizations mitigate the privacy
6 risks associated with information systems and net-
7 works.”.

8 **SEC. 602. NATIONAL PRIVACY AWARENESS AND EDU-**
9 **CATION INITIATIVE.**

10 (a) IN GENERAL.—The Director of the National In-
11 stitute of Standards and Technology, in consultation and
12 collaboration with the Director of the Digital Privacy
13 Agency, relevant Federal agencies, State, local, and Tribal
14 governments, industry, educational institutions, civil soci-
15 ety, and other nonprofit organizations, as appropriate,
16 shall carry out privacy-related education and public aware-
17 ness activities, including relating to the following:

18 (1) The widespread dissemination of privacy-re-
19 lated technical standards and best practices identi-
20 fied by the Director.

21 (2) Efforts to make privacy-related technical
22 standards and best practices usable by individuals,
23 small- to medium-sized businesses, educational insti-
24 tutions, and State, local, and Tribal governments.

1 (3) Activities to increase the awareness of pri-
2 vacy risks, individual privacy rights, and responsibil-
3 ities.

4 (4) Supporting the development of technical
5 standards and best practices to describe privacy-re-
6 lated tasks, knowledge, skills, competencies, and
7 work roles to guide career development, education,
8 and training activities in industry, academia, non-
9 profit organizations, and the Federal Government,
10 including support for credentialing.

11 (b) CONSIDERATIONS.—In carrying out subsection
12 (a), the Director of the National Institute of Standards
13 and Technology, in consultation with appropriate Federal
14 agencies, shall leverage, to the extent practicable, the na-
15 tional cybersecurity awareness and education program
16 under section 303 of the Cybersecurity Enhancement Act
17 of 2014 (15 U.S.C. 7443).

18 (c) BIENNIAL BRIEFINGS.—Not later than one year
19 after the date of the enactment of this Act and biennially
20 thereafter, the Director of the National Institute of Stand-
21 ards and Technology shall brief the Committee on Com-
22 merce, Science, and Transportation of the Senate and the
23 Committee on Science, Space, and Technology of the
24 House of Representatives on the activities carried out pur-
25 suant to subsection (a).

1 (d) AUTHORIZATION OF APPROPRIATIONS.—There is
2 authorized to be appropriated to carry out this section
3 \$3,000,000 for each of fiscal years 2026 through 2030.

4 **SEC. 603. NATIONAL SCIENCE FOUNDATION PRIVACY RE-**
5 **SEARCH.**

6 The Director of the National Science Foundation, in
7 consultation and collaboration with the Director of the
8 Digital Privacy Agency, shall make awards on a competi-
9 tive basis to institutions of higher education or non-profit
10 organizations (or consortia of such institutions or organi-
11 zations) to support multidisciplinary and transdisciplinary
12 socio-technical research to design, prototype, and translate
13 to practice privacy-preserving technologies and increase
14 understanding of the human, social, behavioral, and eco-
15 nomic dimensions of such technologies, including research
16 on the following:

17 (1) Public understanding, expectations, and
18 perspectives on privacy.

19 (2) Consumer privacy rights, including right to
20 access, correction, deletion, data portability, indi-
21 vidual autonomy, impermanence, and to be in-
22 formed.

23 (3) Privacy governance and transparency, in-
24 cluding notice and consent processes and the efficacy
25 of privacy policies.

1 (4) Empowering consumers for data ownership
2 and control.

3 (5) Privacy by design.

4 (6) Privacy-preserving automated decision-mak-
5 ing systems and human review of automated deci-
6 sion-making systems.

7 (7) Ensuring privacy in consumer surveillance
8 systems.

9 (8) User interfaces, including design elements
10 that deliberately obscure, mislead, coerce, or deceive
11 consumers.

12 (9) Privacy implications of emerging tech-
13 nologies.

14 (10) Incentives to implement privacy protec-
15 tions.

○