I

118TH CONGRESS
1ST SESSION

H. R. 2701

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

APRIL 19, 2023

Ms. ESHOO (for herself and Ms. LOFGREN) introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committees on the Judiciary, House Administration, 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.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Online Privacy Act of 2023''.

(b) TABLE OF CONTENTS.—The table of contents for 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. Privacy considerations for legislative branch agencies.
Sec. 6. 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.

SEC. 2. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''Agency'' means the Digital Privacy Agency established in section 301.

(2) AGENCY INVESTIGATOR.—The term ''Agency investigator'' means any attorney or investigator employed by the Agency who is charged with the duty of enforcing or carrying into effect any provision of this Act or a rule or order prescribed under this Act.

(3) BEHAVIORAL PERSONALIZATION.—

(A) IN GENERAL.—The term ''behavioral personalization'' means the processing of an individual's personal information, using an algorithm, model, or other means—

(i) built using—

(I) that individual's personal information collected over a period of time; or

(II) an aggregate of the information of one or more similarly situated individuals; and

(ii) designed to—

(I) alter, influence, guide, or predict that individual's behavior;

(II) tailor or personalize a product or service to that individual; or

(III) filter, sort, limit, promote, display or otherwise differentiate between specific content or categories of content that would otherwise be accessible to that individual.

(B) EXCLUSIONS.—The term ''behavioral personalization'' does not include the use of historical personal information to merely prevent

the display of or provide additional information about previously accessed content.

(4) COLLECT.—The term ''collect'' includes, with respect to personal information or the contents of any communication, obtaining such information or contents in any manner, except when solely transmitting, routing, providing intermediate storage for, or providing connections for such personal information or communication through a system or network.

(5) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(6) CONTENTS.—The term ''contents'', when used with respect to communication, has the meaning given such term in section 2510 of title 18, United States Code.

(7) COVERED ENTITY.—

(A) IN GENERAL.—The term ''covered entity'' means a person who—

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

(ii) sends or receives such personal information over the internet or a similar communications network.

(B) EXCLUSION.—The term ''covered entity'' does not include a natural person, except to

the extent such person is engaged in a commercial activity that is more than de minimis.

(8) CUSTODIAN.—The term ''custodian'' means the custodian or any deputy custodian designated by the Agency.

(9) DATA BREACH.—The term ''data breach'' means unauthorized access to or acquisition of personal information or contents of communications maintained by such covered entity.

(10) DATA-SHARING ABUSE.—The term ''data-sharing abuse'' means processing, by a third party, of personal information or contents of communications disclosed by a covered entity to the third party, for any purpose other than—

(A) a purpose specified by the covered entity to the third party at the time such personal information or contents of communications was disclosed; or

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

(11) DE-IDENTIFY.—

(A) IN GENERAL.—The term ''de-identify'' means, with respect to information, performing actions so that such information cannot reasonably 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.

(12) DIRECTOR.—The term ''Director'' means the Director of the Agency.

(13) DISCLOSE.—The term ''disclose'' means, with respect to personal information or contents of communication, to sell, release, transfer, share, disseminate, make available, or otherwise cause to be communicated, such information or contents to a third party.

(14) DOCUMENTARY MATERIAL.—The term ''documentary material'' includes the original or any copy of any book, document, record, report, memorandum, paper, communication, tabulation, chart, logs, electronic files, or other data or data compilations stored in any medium.

(15) FEDERAL AGENCY.—The term ''Federal agency'' has the meaning given to the term ''agency'' in section 3371 of title 5, United States Code.

(16) FEDERAL PRIVACY LAWS.—The term ''Federal privacy laws'' includes the laws and regulations described in section 502.

(17) GOVERNMENT ENTITY.—The term ''government entity'' means—

(A) a Federal agency;

(B) a State or political subdivision thereof;

(C) or any agency, authority, or instrumentality of a State or political subdivision thereof.

(18) INDIVIDUAL.—The term ''individual'' means a natural person residing in the United States.

(19) INDIAN TRIBE.—The term ''Indian Tribe'' has the meaning given such term in section 4(e) of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304(e)).

(20) MAINTAIN.—The term ''maintain'' means, with respect to personal information or the contents of any communication, to store, secure, or otherwise cause the retention of such information or contents, or to take actions necessary for storing, securing, or otherwise causing the retention of such information or contents.

(21) NONPUBLIC INFORMATION.—The term ''nonpublic information'' means information that has not been disclosed in a criminal, civil, or administrative proceeding, in a government investigation, report, or audit, or by the news media or other public source of information, and that was not obtained in violation of the law.

(22) PERSONAL INFORMATION.—

(A) IN GENERAL.—The term ''personal information'' means any information maintained by a covered entity that, on its own or com-

bined with other information, is linked or reasonably linkable to a specific individual or a specific device, including de-identified personal information and the means to behavioral personalization created for or linked to a specific individual.

(B) EXCLUSIONS.—The term ''personal information'' does not include—

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

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

(23) PRIVACY HARM.—The term ''privacy harm'' means an adverse consequence or a potential adverse consequence to an individual, a group of individuals, or society caused from collecting, processing, maintaining, or disclosing of personal information or contents of communications, including—

(A) direct or indirect financial loss or economic harm;

(B) physical harm;

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

(D) adverse outcomes or decisions with respect to the eligibility of an individual for rights, benefits, or privileges in employment (including hiring, firing, promotion, demotion, and compensation), credit and insurance (including denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services;

(E) stigmatization or reputational harm;

(F) price discrimination;

(G) adverse consequences that affect the private life of an individual, including private family matters and actions and communications within the home of such individual or a similar physical, online, or digital location where such individual has a reasonable expectation that personal information will not be collected, processed, or maintained;

(H) the chilling of free expression or action of an individual, a group of individuals, or society, due to perceived or actual pervasive and excessive collecting, processing, disclosing, or maintaining of personal information or contents of communications;

(I) impairing the autonomy of an individual, a group of individuals, or society; and

(J) other adverse consequences or potential adverse consequences, consistent with the provisions of this Act, as determined by the Director.

(24) PRIVACY-PRESERVING COMPUTING.—

(A) IN GENERAL.—The term ''privacy-preserving computing'' means the collecting, processing, disclosing, or maintaining of personal information that has been encrypted or otherwise rendered unintelligible using a means that cannot be reversed by a covered entity, or a covered entity's service provider, such that—

(i) if such personal information could be rendered intelligible through cooperation or sharing of cryptographic secrets by multiple persons, the covered entity has both technical safeguards and business processes to prevent such cooperation or sharing;

(ii) if such personal information is rendered intelligible within a hardware processing unit or other means of performing operations on the information,

there are technical safeguards that, during the normal course of operation—

(I) prevent rendering personal information intelligible anywhere but within the hardware processing unit or other means of performing operations; and

(II) make the exporting or otherwise observing of such intelligible information, or the cryptographic secret used to protect such information, impossible; and

(iii) if the result of such processing of the personal information is also personal information, such result must be unintelligible to the covered entity or service provider and protected by privacy-preserving computing.

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

(25) PROCESS.—The term ''process'' means to perform or cause to be performed any operation or set of operations on personal information or contents

of communication, whether or not by automated means.

(26) PROTECTED CLASS.—The term ''protected class'' means the actual or perceived race, color, ethnicity, national origin, religion, sex (including sexual orientation and gender identity or expression), familial status, or disability of an individual or group of individuals.

(27) PUBLICLY AVAILABLE INFORMATION.—The term ''publicly available information''—

(A) means—

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

(ii) information linked to a public individual or official that is made publicly accessible, without restrictions on accessibility other than the general authorization to access the services used to make the information accessible;

(iii) information of an individual that—

(I) is made publicly accessible by such individual, without restrictions on accessibility other than the general authorization to access the services

used to make the information accessible; and

(II) such individual has the ability to delete or change without relying on a request under section 102 or 103; and

(B) does not include—

(i) biometric information of an individual collected by a covered entity without the individual's knowledge;

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

(iii) information obtained from government records for the purpose of selling such information; or

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

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

(A) is equivalent in availability and ease of use to that of other mechanisms for communicating or interacting with the covered entity; and

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

(29) SELL AND SALE.—

(A) IN GENERAL.—The terms ''sell'' and ''sale'' mean the disclosing of personal information for monetary consideration or for a thing of value by a covered entity to a third party for the purposes of processing, maintaining or disclosing such personal information at the third party's discretion.

(B) EXCLUSIONS.—The terms ''sell'' and ''sale'' do not include—

(i) the disclosing of personal information of an individual to a third party with which the individual has a direct relation-

ship for purposes of providing a product or service requested by the individual or otherwise in a manner that is consistent with an individual's reasonable expectations considering the context in which the individual provided the personal information to the covered entity;

(ii) the disclosing or transfer of personal information to a subsidiary or an affiliate of the covered entity; or

(iii) the disclosing or transfer of personal information to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the covered entity's assets, unless personal information makes up the majority of the value of the assets of which the third party assumes control.

(30) SERVICE PROVIDER.—

(A) IN GENERAL.—The term ''service provider'' means a covered entity that—

(i) processes, discloses, or maintains personal information, where such covered entity does not process, disclose, or main-

tain the personal information other than in accordance with the directions and on behalf of another covered entity;

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

(iii) does not earn revenue from processing, maintaining, or disclosing personal information disclosed to such covered entity by another covered entity except by providing contracted services to such other covered entity;

(iv) does not disclose personal information to another covered entity unless such personal information was provided by such other covered entity or resulted from maintaining or processing performed on personal information exclusively provided by such other covered entity;

(v) does not offer services that allow another covered entity to target specific individuals using personal information not provided by such other covered entity;

(vi) with respect to personal information processed or maintained by such covered entity on behalf of another covered entity, assists such other covered entity in complying with title I, including providing tools for such other covered entity to comply with such requirements if requested; and

(vii) does not link the personal information provided by another covered entity to personal information from any other source.

(B) TREATMENT.—A covered entity shall be treated as a service provider under this Act only to the extent that such covered entity is acting as a service provider, as defined in subparagraph (A).

(31) SIGNIFICANT PRIVACY HARM.—The term ''significant privacy harm'' means adverse consequences to an individual arising from the collecting, processing, maintaining, or disclosing of personal information or contents of communications, limited to subparagraph (A), (B), or (D) of paragraph (23).

(32) SMALL BUSINESS.—The term ''small business'' means a covered entity that—

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

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

(C) has not, in combination with each subsidiary and affiliate of the service, maintained personal information of 250,000 or more individuals for 3 or more of the preceding 12 months;

(D) has fewer than 200 employees; and

(E) received less than $25,000,000 in gross revenue in the preceding 12-month period.

(33) STATE.—The term ''State'' means each State of the United States, the District of Columbia, each commonwealth, territory, or possession of the United States, and each federally recognized Indian Tribe.

(34) STATE ATTORNEY GENERAL.—The term ''State attorney general'' means, with respect to a State, the attorney general or chief law enforcement officer of the State, or another official or agency

designated by the State to bring civil actions on behalf of the State or the residents of the State.

(35) STATE PRIVACY REGULATOR.—The term ''State privacy regulator'' means an agency or instrumentality of a State that has the primary purpose of administering, implementing, or enforcing a privacy law or associated rules or regulations.

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

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

(B) that is not—

(i) such covered entity;

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

(iii) a service provider of such covered entity.

(37) USERS.—The term ''users'' means, with respect to a product or service, the monthly active users, subscribers, or customers (or a reasonable proxy or substitute therefor determined by the Director) of such product or service.

(38) VIOLATION.—The term ''violation'' means, except where otherwise specified, any act or omission that, if proved, would constitute a violation of any

provision of this Act or a rule or order issued pursuant to this Act.

SEC. 3. GENERAL PROVISIONS.

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

(1) any reference to information as being of or belonging to an individual shall be construed to mean that such information is linked or reasonably linkable to such individual as described in section 2(21)(A); and

(2) any reference to any communication as being of or belonging to an individual shall be construed to mean that such individual is party to such communication.

(b) PROHIBITION ON WAIVERS.—

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

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

(c) JOURNALISM PROTECTION.—

(1) IN GENERAL.—Covered entities engaged in journalism shall not be subject to the obligations imposed under this Act to the extent that those obligations directly infringe on the journalism rather than the business practices of the covered entity, so long as the covered entity has technical safeguards and business processes that prevent the collecting, processing, maintaining, or disclosing of such personal information for business practices other than journalism.

(2) JOURNALISM.—The term ''journalism'' includes the collecting, maintaining, processing, and disclosing of personal information about a public individual or official, or that otherwise concerns matters of public interest, for dissemination to the public.

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

(e) PROHIBITION ON COLLECTING, MAINTAINING, PROCESSING, OR DISCLOSING PERSONAL INFORMATION.—A covered entity may not collect, maintain, process, or disclose personal information using a channel of

interstate commerce unless such covered entity is in compliance with all requirements of this Act.

SEC. 4. LIMITATION ON DISCLOSING NONREDACTED GOVERNMENT RECORDS.

(a) IN GENERAL.—A government entity may not use a channel of interstate commerce to disclose the personal information of an individual in a government record without an agreement prohibiting the recipient of such information from selling the information without the express consent of the individual.

(b) EXCEPTION.—Notwithstanding subsection (a), nothing in this section shall prohibit the disclosure of personal information using a channel of interstate commerce to another government entity without consent of the individual.

SEC. 5. PRIVACY CONSIDERATIONS FOR LEGISLATIVE BRANCH AGENCIES.

(a) GOVERNMENT PUBLISHING OFFICE.—

(1) PRIVACY RESPONSIBILITIES OF THE DIRECTOR.—

(A) IN GENERAL.—Chapter 3 of title 44, United States Code, is amended by inserting at the end the following:

"§ 319. Privacy responsibilities of the Director of the Government Publishing Office

''The Director of the Government Publishing Office shall identify and implement appropriate measures to prevent the disclosure of personal information by the Government Publishing Office and to minimize the risk of privacy harms in its operations.''.

(B) CLERICAL AMENDMENT.—The table of sections for chapter 3 of title 44, United States Code, is amended by inserting after the item relating to section 318 the following:

''319. Privacy responsibilities of the Director of the Government Publishing Office.''.

(2) PRIVACY SAFEGUARDS FOR PUBLISHED DOCUMENTS.—Section 1701 of title 44, United States Code, is amended by striking ''the publication.'' in the last sentence of the first paragraph and inserting ''the publication, and only after conducting an appropriate review or implementing other appropriate measures to prevent the disclosure of personal information and minimize the risks of privacy harms in such publication.''.

(3) PRIVACY SAFEGUARDS IN THE DEPOSITORY LIBRARY PROGRAM.—Section 1902 of title 44, United States Code, is amended by inserting at the end the following: ''The Superintendent of Docu-

ments shall assess the risks of disclosure of personal information and related privacy harms in publications made available to and by depository libraries and shall implement appropriate measures to minimize such risks, including to the extent necessary by imposing obligations upon depository libraries.''.

(b) LIBRARY OF CONGRESS.—The first paragraph under the center heading ''LIBRARY OF CONGRESS'' under the center heading ''LEGISLATIVE'' of the Act entitled ''An Act Making appropriations for the legislative, executive, and judicial expenses of the Government for the fiscal year ending June thirtieth, eighteen hundred and ninety-eight, and for other purposes'', approved February 19, 1897 (2 U.S.C. 136), is amended by striking at the end ''Library.'' and inserting ''Library, including by identifying and implementing appropriate measures to prevent the disclosure of personal information by the Library and to minimize the risk of privacy harms in its operations.''.

(c) SMITHSONIAN INSTITUTION.—Section 7 of the Act entitled ''An Act to establish the 'Smithsonian Institution' for the increase and diffusion of knowledge among men'', approved August 10, 1846 (20 U.S.C. 46), is amended by adding at the end the following: ''The Secretary shall assess the risks of disclosure of personal information by the institution and related privacy harms and

shall implement appropriate measures to minimize such risks.''.

(d) CHIEF ADMINISTRATIVE OFFICER OF THE HOUSE OF REPRESENTATIVES.—

(1) IN GENERAL.—Subchapter III of chapter 55 of title 2, United States Code, is amended by inserting at the end the following:

''§ 5549. Privacy responsibilities

''The Chief Administrative Officer of the House of Representatives shall identify and implement appropriate measures to prevent the disclosure of personal information and to minimize the risk of privacy harms in its areas of operational and financial responsibility.''.

(2) CLERICAL AMENDMENT.—The table of sections for subchapter III of chapter 55 of title 2, United States Code, is amended by inserting after the item relating to section 5548 the following:

''5549. Privacy responsibilities.''.

SEC. 6. CRIMINAL PROHIBITION ON DOXXING.

(a) IN GENERAL.—Chapter 41 of title 18, United States Code, is amended by adding at the end the following:

"§ 881. Disclosing of personal information with the intent to cause harm

''(a) IN GENERAL.—Whoever uses a channel of interstate or foreign commerce to knowingly disclose an individual's personal information with the intent—

''(1) to threaten, intimidate, or harass any person, incite or facilitate the commission of a crime of violence against any person, or place any person in reasonable fear of death or serious bodily injury; or

''(2) that the information will be used to threaten, intimidate, or harass any person, incite or facilitate the commission of a crime of violence against any person, or place any person in reasonable fear of death or serious bodily injury,

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

''(b) DEFINITIONS.—In this section:

''(1) CONTENTS.—The term 'contents' when used with respect to communication, has the meaning given such term in section 2510 of title 18, United States Code.

''(2) DISCLOSE.—The term 'disclose' means, with respect to personal information or contents of communication, to sell, release, transfer, share, disseminate, make available, or otherwise cause to be

communicated such information or contents to a third party.

''(3) GOVERNMENT ENTITY.—The term 'government entity' means—

''(A) a Federal agency (as such term is defined in section 3371 of title 5, United States Code);

''(B) a State or political subdivision thereof; or

''(C) any agency, authority, or instrumentality of a State or political subdivision thereof.

''(4) INDIVIDUAL.—The term 'individual' means a natural person residing in the United States.

''(5) PERSONAL INFORMATION.—

''(A) IN GENERAL.—The term 'personal information' means any information maintained by a person that, on its own or combined with other information, is linked or reasonably linkable to a specific individual.

''(B) EXCLUSIONS.—The term 'personal information' does not include—

''(i) publicly available information linked to an individual; or

''(ii) information derived or inferred from personal information, if the derived

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

''(6) PUBLICLY AVAILABLE INFORMATION.—The term 'publicly available information'—

''(A) means—

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

''(ii) information linked to a public individual or official that is made publicly accessible, without restrictions on accessibility other than the general authorization to access the services used to make the information accessible;

''(iii) information of an individual that—

''(I) is made publicly accessible by such individual, without restrictions on accessibility other than the general authorization to access the services used to make the information accessible; and

''(II) such individual has the ability to delete or change; and

''(B) does not include—

''(i) biometric information of an individual collected by a covered entity without the individual's knowledge;

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

''(iii) information obtained from government records for the purpose of selling such information; or

''(iv) information used to contact or locate a private individual either physically or electronically.

''(7) STATE.—The term 'State' means each State of the United States, the District of Columbia, each commonwealth, territory, or possession of the United States, and each federally recognized Indian Tribe.''.

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

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

TITLE I—INDIVIDUAL RIGHTS

SEC. 101. RIGHT OF ACCESS.

(a) IN GENERAL.—A covered entity shall make available a reasonable mechanism by which an individual may access—

(1) the categories of personal information and contents of communications of such individual that is maintained by such covered entity, including, in the case of personal information that such covered entity did not collect from such individual, how and from whom such covered entity obtained such personal information;

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

(3) a concise and clear description of the business or commercial purposes of such covered entity—

(A) for collecting, processing, or maintaining the personal information of such individual; and

(B) for disclosing to a third party the personal information of such individual; and

(4) a list of automated decision-making processes that an individual has a right to request human review of under section 105 with a concise and clear description of the implications and intended effects of each such process.

(b) EXCEPTION FOR PUBLICLY ACCESSIBLE INFORMATION.—A covered entity that makes available information required in subsection (a) shall be considered in compliance with such requirements if the covered entity provides an individual with instructions on how to access a public posting of such information, including in a privacy policy, if the instructions are easy and do not require payment.

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

SEC. 102. RIGHT OF CORRECTION.

(a) DISPUTE BY INDIVIDUAL.—A covered entity shall make available a reasonable mechanism by which an individual may dispute the accuracy or completeness of personal information linked to such individual that is maintained by such covered entity if such information is processed in any way, by such covered entity, a third party of such covered entity, or a service provider of such covered entity that may increase reasonably foreseeable significant privacy harms.

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

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

(2) notify such individual that—

(A) the disputed information is correct or complete;

(B) such covered entity lacks sufficient information to correct or complete the disputed information; or

(C) such covered entity is denying the request for correction or completion in reliance on an exemption or exception provided by section 109(g).

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

SEC. 103. RIGHT OF DELETION.

(a) REQUEST BY INDIVIDUAL.—A covered entity shall make available a reasonable mechanism by which an individual may request the deletion of personal information and contents of communications of such individual maintained by such covered entity, including any such information that such covered entity acquired from a third

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

(b) DELETION BY COVERED ENTITY.—A covered entity receiving a request for deletion under subsection (a) shall—

(1) delete such information and notify such individual that such information has been deleted; or

(2) notify such individual that such covered entity is denying the request for deletion in reliance on an exemption or exception provided by section 109(g).

SEC. 104. RIGHT OF PORTABILITY.

(a) DETERMINATION OF PORTABLE CATEGORIES.—

(1) ANNUAL DETERMINATION.—Not less frequently than once per calendar year, the Director shall—

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

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

(C) publish in the Federal Register a list of portable categories determined under subparagraph (B).

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

(A) publish a draft of such list in the Federal Register; and

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

(b) EXERCISE OF RIGHT.—

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

(A) download, in a format that is structured, commonly used, and machine readable—

(i) any such personal information that such individual has provided to such covered entity, with the option to download such information by category that is accessible under section 101; and

(ii) the contents of any such communications; and

(B) using a real-time application programming interface, or similar mechanism, transmit

all such personal information (whether or not provided to such covered entity by such individual) and the contents of any such communication from such covered entity to another covered entity in accordance with subsection (c).

(2) REQUIREMENTS FOR APPLICATION PROGRAMMING INTERFACE.—The application programming interface, or similar mechanism, required by paragraph (1)(B) shall—

(A) be publicly documented;

(B) allow the option of obtaining any personal information of an individual that the individual has provided to the covered entity, if such information is accessible under section 101;

(C) include a publicly available, fully functional test version for development purposes; and

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

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

(1) ACCESS.—Except as provided in paragraph (2)(A), a covered entity shall provide access to the

application programming interface or similar mechanism required by subsection (b)(1)(B) upon the request of another covered entity if the requesting covered entity has self-certified, using the procedures established by the Director under paragraph (3)(A), that such requesting covered entity—

(A) is a covered entity;

(B) can have personal information disclosed to it under section 204;

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

(D) will continue to comply with all requirements of this Act; and

(E) will only use such application programming interface or similar mechanism at the express request of an individual.

(2) DENIAL OF ACCESS.—

(A) IN GENERAL.—A covered entity may deny access to the application programming interface or similar mechanism required by subsection (b)(1)(B) if such covered entity has an objective, reasonable belief that the requesting

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

(B) REVIEW.—In accordance with the procedures established under paragraph (3)(B), a covered entity the request of which is denied under subparagraph (A) may petition the Director for review of the denial. If the Director finds that such denial is unreasonable, the Director shall impose a penalty, to be established in such procedures, on the covered entity that denied the request.

(3) CERTIFICATION AND REVIEW PROCEDURES.—The Director shall establish—

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

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

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

(e) PORTABLE CATEGORY DEFINED.—In this section, the term ''portable category'' means a category of products and services established by the Director under subsection (a)(1)(A)—

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

(2) that—

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

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

(C) the Director otherwise determines that a category would benefit from encouraging increased competition.

SEC. 105. RIGHT TO HUMAN REVIEW OF AUTOMATED DECISIONS.

For any decision by a covered entity based solely on automated processing of personal information of an individual, if such processing materially increases reasonably foreseeable significant privacy harms for such individual, such covered entity shall—

(1) inform such individual of what personal information is being or may be used for such decision;

(2) make available a reasonable mechanism by which such individual may request human review of such decision, upon request or in a publicly accessible location; and

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

SEC. 106. RIGHT TO INDIVIDUAL AUTONOMY.

(a) IN GENERAL.—A covered entity shall not collect, process, maintain, or disclose an individual's personal information to—

(1) create, improve upon, or maintain;

(2) process with; or

(3) otherwise link an individual with;

an algorithm, model, or other means designed for behavioral personalization, without the affirmative express consent of that individual.

(b) CONSENT.—A covered entity must obtain express affirmative consent from an individual before it may provide a behaviorally personalized version of a product or service, and not less than every calendar year thereafter. Where consent is denied, a covered entity must provide the product or service without behavioral personalization.

(c) EXCEPTIONS TO PROVIDING PRODUCT OR SERVICE.—

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

product or service that can be offered without behavioral personalization.

(2) Where no core aspect or part of the product or service can function in a substantially similar function without behavioral personalization, a covered entity may deny providing an individual use of such product or service if such individual does not consent to behavioral personalization as required in subsection (a).

(d) EXCEPTION TO BEHAVIORAL PROCESSING.—Notwithstanding subsections (a) and (b), a covered entity may process personal information to create or operate behavioral personalization algorithms, models, or other mechanisms for the purpose of increasing the usability of the product or service provided by a covered entity that—

(1) are built using aggregated personal information that is representative of all the personal information the covered entity maintains; and

(2) have an output that is both uniform across the individuals that use the product or service and independent of a specific individual's inherent or behavioral characteristics.

(e) USABILITY.—The term ''usability'' as used in subsection (d) does not include optimizations or other alterations to the product or service that are made with the

primary purpose of increasing the amount of time an individual engages with or uses the product or service, unless such increase benefits the individual.

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

SEC. 107. RIGHT TO BE INFORMED.

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

SEC. 108. RIGHT TO IMPERMANENCE.

(a) LIMITATION ON MAINTAINING OF PERSONAL INFORMATION.—A covered entity shall not maintain personal information for more time than expressly consented to by an individual whose personal information is being maintained.

(b) CONSENT.—A covered entity must obtain express affirmative consent from an individual before maintaining the personal information of such individual for any duration. Such consent may be obtained for categories of personal information and shall give an individual options to

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

(1) for no longer than needed to complete the specific request or transaction (including a reasonable estimate of such duration by the covered entity);

(2) until consent is revoked; and

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

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

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

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

(1) IN GENERAL.—This title does not apply with respect to personal information that is collected, processed, maintained, or disclosed for any of the following purposes (or a combination of such

purposes), where a covered entity has technical safeguards and business processes that limit collecting, processing, maintaining, or disclosing of such personal information to the following purposes:

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

(B) Protecting against malicious, deceptive, fraudulent, or illegal activity.

(C) A good faith response to, or compliance with, a valid subpoena, court order, or warrant (including a subpoena and court order obtained by an entity that is not a government entity) or otherwise providing information as required by law.

(D) Protecting a legally recognized privilege or other legal right.

(E) Protecting public safety.

(F) Collecting, processing, or maintaining by an employer pursuant to an employer-employee relationship of records about employees or employment status, except—

(i) where the information would not be reasonably expected to be collected in the context of an employee's regular duties; or

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

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

(H) Routing a communication through a communications network or resolving the location of a host or client on a communications network.

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

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

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

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

(B) a description of the rights provided by this title that are not available with respect to such personal information by reason of such exemption.

(b) EXCEPTIONS FOR PARTICULAR REQUESTS.—

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

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

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

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

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

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

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

(ii) was collected specifically for the completion of such transaction or the performance of such contract; and

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

(2) LIMITATIONS ON REQUESTS FOR ADDITIONAL INFORMATION TO CONFIRM IDENTITY.—A covered entity may not deny a request of an individual under paragraph (1)(A) on the basis of the refusal of such individual to provide additional personal information to such covered entity to confirm the identity of such individual—

(A) if the identity of such individual can reasonably be confirmed using personal information of such individual that such covered entity (as of the time of the request) already maintains; or

(B) if such individual has an existing relationship (as of the time of the request) with such covered entity, such individual has confirmed the identity of such individual to such covered entity in the same manner as for other transactions of a similar sensitivity.

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

(d) EXEMPTION FOR PRIVACY-PRESERVING COMPUTING.—Except for sections 101, 105, and 106, this title does not apply to personal information secured using privacy-preserving computing.

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

(1) comply with such request; or

(2) inform such individual of the reason for denying such request, as allowed under subsection (a) or (b).

(f) FEES PROHIBITED.—

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

(2) UNFOUNDED OR EXCESSIVE REQUESTS.—If a request under this title is unfounded or excessive, a covered entity may charge a reasonable fee that reflects the estimated administrative costs of complying with such request.

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

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

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

(B) such request is not unfounded or excessive.

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

(1) take an action that would convert information that is not personal information into personal information;

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

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

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

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

SEC. 201. MINIMIZATION.

(a) ARTICULATED BASIS.—A covered entity shall have a reasonable, articulated basis for collecting, processing, maintaining, and disclosing of personal information that takes into account the reasonable business needs of the covered entity and minimum amount of personal information necessary for providing the service, balanced with the intrusion on the privacy of, potential privacy harms to, and reasonable expectations of individuals to whom the personal information relates.

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

(1) COLLECTING.—A covered entity may not collect more personal information than is reasonably needed to provide a product or service that an individual has requested.

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

which is in accordance with the directions of a covered entity.

(3) MAINTAINING.—A covered entity may not maintain personal information once such information is no longer needed for the purpose for which such information was originally collected from the individual or in the case of a service provider, a purpose other than that which is in accordance with the directions of a covered entity.

(4) DISCLOSING.—A covered entity may not disclose personal information for a purpose other than the purpose for which such information was originally collected from the individual or in the case of a service provider, a purpose other than that which is in accordance with the directions of a covered entity.

(c) ANCILLARY COLLECTING, PROCESSING, MAINTAINING, AND DISCLOSING.—Notwithstanding subsection (b), a covered entity may collect, process, disclose, or maintain personal information beyond limitations under subsection (b) only if such covered entity complies with this subsection.

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

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

(2) NOTICE REQUIRED.—A covered entity shall provide notice of ancillary collecting, processing, maintaining, or disclosing of personal information in the case of one, but not more than one, of the following instances:

(A) Such ancillary collecting, processing, maintaining, or disclosing may result in additional or increased privacy harms (but not increased significant privacy harms), and is substantially similar to the purpose for which such personal information was originally collected.

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

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

tional or increased privacy harms (but not increased significant privacy harms) and the purpose is not substantially similar to the purpose for which such personal information was originally collected, so long as the personal information is secured using privacy-preserving computing.

(3) NOTICE AND CONSENT REQUIRED.—For scenarios not covered under paragraph (1) or (2), and notwithstanding sections 208(b)(2) and (3), a covered entity shall provide notice of and obtain consent for ancillary collecting, processing, maintaining, or disclosing of personal information.

(d) SUBSTITUTION.—In cases in which personal information can be replaced with artificial personal information, personal information that has been de-identified, or the random personal information of one or more individuals without substantially reducing the utility of the data or requiring an unreasonable amount of effort, such a replacement shall take place.

SEC. 202. MINIMIZATION AND RECORDS OF ACCESS BY EMPLOYEES AND CONTRACTORS.

(a) MINIMIZATION.—A covered entity shall restrict access to personal information and contents of communications by the employees or contractors of such covered

entity based on an articulated balance between the potential for privacy harm, reasonable expectations of individuals to whom the personal information relates, and reasonable business needs.

(b) RECORDS OF ACCESS.—

(1) IN GENERAL.—A covered entity shall maintain records identifying each instance in which an employee or a contractor of such covered entity accesses personal information or contents of communications if disclosing such personal information or contents of communication, or a data breach or data-sharing abuse involving such personal information or contents of communication, may foreseeably result in increased privacy harms.

(2) INFORMATION REQUIRED.—The records required by paragraph (1) shall include the following:

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

(B) The date and time of access.

(C) The fields of information accessed.

(D) The individuals whose personal information was accessed or the contents of whose communications were accessed.

(3) SMALL BUSINESSES EXCLUDED.—This subsection does not apply to a small business.

SEC. 203. PROHIBITIONS ON DISCLOSING OF PERSONAL INFORMATION.

(a) CONSENT FOR DISCLOSING REQUIRED.—

(1) IN GENERAL.—A covered entity may not intentionally disclose personal information unless the covered entity obtains consent of the individual whose personal information is being disclosed for each category of third party to which such personal information will be disclosed. Such covered entity must also provide such individual with notice of—

(A) each category of third party;

(B) the personal information to be disclosed; and

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

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

(A) IN GENERAL.—A covered entity may not intentionally sell personal information unless the covered entity—

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

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

(B) DISCLOSING SERVICES.—Subparagraph (A) shall not apply to a covered entity in a case in which an individual is directing the covered entity to disclose the personal information of such individual for the sole purpose of procuring goods or services, or offers for goods or services, for such individual, if there is a reasonable mechanism for the individual to withdraw consent.

(3) REQUIREMENT TO INCLUDE ORIGINAL PURPOSE OF COLLECTING.—A covered entity may not intentionally disclose personal information without including the purpose for which the personal information was originally collected.

(4) EXCEPTION FOR PRIVACY-PRESERVING COMPUTING.—Notwithstanding paragraph (1), consent is not required for disclosing (not including sell-

ing) personal information secured using privacy-preserving computing.

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

(A) re-identification of the disclosed personal information; and

(B) the processing of additional personal information in combination with the disclosed personal information that would allow for the re-identification of the disclosed personal information.

(b) DISCLOSING FOR ADVERTISING OR MARKETING PURPOSES.—

(1) IN GENERAL.—A covered entity may not intentionally disclose for advertising or marketing purposes a unique identifier or any other personal information that would allow information disclosed to be linked to information relating to the same individual or device disclosed in the past.

(2) TREATMENT OF CERTAIN TYPES OF INFORMATION.—Disclosing personal information or contents of communication for advertising or marketing purposes may not be treated as violating paragraph (1) by reason of including any or all of the following:

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

(B) Geolocation information truncated to allow no more than the equivalent of two decimal degrees of precision at the equator or prime meridian, or an equivalent precision in another geolocation standard.

(C) A general description of a device, browser, or operating system, or any combination thereof.

(D) An identifier that is unique to a disclosure.

SEC. 204. DISCLOSING TO ENTITIES NOT SUBJECT TO UNITED STATES JURISDICTION OR NOT COMPLIANT WITH THIS ACT.

(a) PROHIBITION.—A covered entity may not intentionally disclose personal information to any entity that—

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

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

(b) EXCEPTION.—Notwithstanding subsection (a), a covered entity may disclose personal information where that personal information is limited to an identifier created primarily for the purpose of sending or receiving electronic communications and the sole purpose of disclosing is to send or receive an electronic communication at the request of the individual whose personal information is being disclosed.

(c) SAFE HARBORS FOR DISCLOSING.—Notwithstanding subsection (a), a covered entity may disclose personal information to another covered entity (the receiving covered entity) that is not subject to the jurisdiction of the United States if either—

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

(A) the covered entity has a reasonable belief that the receiving covered entity is sufficiently solvent to compensate victims or pay fines for violations of this Act;

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

(C) a contract between the covered entity and the receiving covered entity prohibits the receiving covered entity from using the disclosed personal information for any purpose other than provided in the contract; or

(2) the covered entity has—

(A) entered into an agreement with the receiving covered entity that—

(i) requires the receiving covered entity to comply with this Act;

(ii) prohibits the receiving covered entity from using the disclosed personal information for any purpose other than provided in the contract;

(iii) requires the receiving covered entity to indemnify the covered entity against violations of this Act committed by the receiving covered entity for any amount the covered entity is unable to pay of a judgment for such violation;

(iv) grants the covered entity the authority to audit, including physical access to electronic devices and data, the receiving covered entity's compliance with this Act and the contract; and

(v) requires the receiving covered entity to assist the covered entity in responding to and complying with any court orders, Agency orders, or the exercising of an individual's rights under this Act;

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

(C) actual knowledge that the receiving covered entity is sufficiently solvent to compensate victims or pay fines for violations of this Act;

(D) an auditing and compliance program to ensure the receiving covered entity's continued compliance with this Act and contract terms;

(E) filed with the Agency the terms of said contract, proof of its actual knowledge of the receiving covered entity's compliance with this Act and contract terms, and documents detailing its auditing and compliance program for approval and publication by the Agency; and

(F) entered into an agreement with the Agency where the covered entity agrees to accept, respond to, or comply with a court order, Agency order, or request by an individual regarding actions taken by the receiving covered entity with respect to covered information it has disclosed.

(d) LIABILITY FOR VIOLATION BY RECEIVING COVERED ENTITY; FAILURE TO REPORT.—For the purposes of subsection (c)(2), the covered entity shall be jointly liable for a violation of this Act by the receiving covered entity regarding the personal information the covered entity disclosed, except where the covered entity was the first to notify the Agency of the violation, in which case, it shall be severally liable. Where the covered entity should reason-

ably have known of a violation of this Act by the receiving covered entity and fails to disclose the violation to the Agency, each day of continuance of the failure to report such violation shall be treated as a separate violation.

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

(1) The principal place of business for the covered entity must be in a country that allows for the domestication of a United States court decision for civil fines payable to a government entity and injunctive relief. Where a foreign court refuses to enforce a United States court decision under this Act, the agreement, and all other agreements with covered entities with a principal place of business in the same jurisdiction, shall be void.

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

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

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

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

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

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

(f) RULE OF CONSTRUCTION AGAINST DATA LOCALIZATION.—Nothing in this section shall be construed to require the localization of processing or maintaining personal information by a covered entity to within the United States, or limit internal disclosing of personal information within a covered entity or to subsidiary or corporate affiliate of such covered entity, regardless of the country in which the covered entity will process, disclose, or maintain that personal information.

SEC. 205. PROHIBITION ON RE-IDENTIFICATION.

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

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

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

SEC. 206. RESTRICTIONS ON COLLECTING, PROCESSING, MAINTAINING, AND DISCLOSING CONTENTS OF COMMUNICATIONS.

(a) IN GENERAL.—A covered entity may not collect, process, maintain, or disclose the contents of any communication, regardless of whether the sender or intended recipient of the communication is an individual, other person, or an electronic device, for any purpose other than—

(1) transmitting or displaying the communication to any intended recipient or the original sender, or maintaining such communications for such purposes;

(2) detecting, responding to, or preventing security incidents or threats;

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

(4) processing expressly requested by the sender or intended recipient, if the sender or intended recipient can terminate such processing using a reasonable mechanism;

(5) disclosing otherwise required by law;

(6) filtering a communication where primary purpose of the communication is the commercial advertisement or promotion of a commercial product or service of a covered entity; or

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

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

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

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

(3) a purpose of the covered entity's service is to maintain, at the direction of the sender, the content of said communication for more than a transitory period.

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

(1) Where the sender is a natural person, they shall be the sender of the entire content of the communication, regardless of the original author of any portion of the content.

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

(d) EXCEPTION FOR PUBLICLY AVAILABLE COMMUNICATIONS.—Subsection (a) shall not apply where the contents of communication are made publicly accessible by the sender without restrictions on accessibility other than the general authorization to access the services used to make the information accessible.

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

(1) prohibit or prevent a person from encrypting or otherwise rendering unintelligible the content of a communication using a means that prevents the covered entity from being able to decrypt or otherwise render intelligible said content; and

(2) require or cause a person to disclose or circumvent the means described in paragraph (1) to the covered entity that would allow it to render the content intelligible.

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

SEC. 207. PROHIBITION ON DISCRIMINATORY PROCESSING.

(a) DISCRIMINATION IN ECONOMIC OPPORTUNITIES.—A covered entity shall not process personal information or contents of communication for advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for employment, finance, health care, credit, insurance, housing, or education opportunities in a manner that discriminates against or otherwise makes opportunities unavailable on the basis of an individual's protected class status.

(b) PUBLIC ACCOMMODATIONS.—A covered entity shall not process personal information in a manner that segregates, discriminates in, or otherwise makes unavailable the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation on the basis of the protected class status of an individual or a group of individuals.

(c) REGULATIONS.—The Director shall promulgate regulations to implement this section.

SEC. 208. REQUIREMENTS FOR NOTICE AND CONSENT PROCESSES AND PRIVACY POLICIES.

(a) MINIMUM THRESHOLD.—The Director shall establish minimum thresholds that covered entities must meet for the percentage of individuals who understand a notice or consent process or privacy policy required by this Act. In establishing such minimum thresholds, the Director shall—

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

(2) take into account expectations of individuals, potential privacy harms, and individuals' awareness of privacy harms.

(b) CONSENT REVOCATION.—A covered entity shall make available a reasonable mechanism by which an indi-

vidual may revoke consent for any consent given under this Act.

(c) SAFE HARBOR.—

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

(2) PRESUMPTION.—If a covered entity submits testing data to and receives an approval from the Director under paragraph (1) establishing that a notice or consent process or privacy policy of such covered entity meets the threshold established under subsection (a), such notice or consent process or privacy policy shall be presumed to have met such threshold. Such presumption may be rebutted by clear and convincing evidence.

(3) PUBLIC AVAILABILITY OF APPROVED PROCESSES AND POLICIES AND ASSOCIATED TESTING DATA.—The Director shall make publicly available online the notice and consent processes and privacy policies and associated testing data that the Director approves under paragraph (1).

(4) SMALL BUSINESS ADOPTION OF NOTICE OR CONSENT PROCESS OF ANOTHER COVERED ENTITY.—

(A) IN GENERAL.—If a small business adopts a notice or consent process of another covered entity that collects, processes, maintains, or discloses personal information in substantially the same way as such small business, if the process of such other covered entity has been approved under paragraph (1), the process of such small business shall receive the presumption under paragraph (2).

(B) ABILITY TO FREELY USE APPROVED PROCESS.—A covered entity whose notice or consent process is approved under paragraph (1) shall permit a small business to freely use such process, or a derivative thereof, as described in subparagraph (A).

(C) NO PUBLISHED PROCESS.—In the case of a small business for which there is no approved notice or consent process published under paragraph (3) of a covered entity that collects, processes, maintains, or discloses personal information in substantially the same way as such small business, any requirement under

this title for a notice or consent process to be objectively shown to meet the threshold established by the Director under subsection (a) shall not apply to such small business. Nothing in the preceding sentence exempts a small business from the requirement to use such notice or consent process or that such process be concise and clear.

(D) INAPPLICABILITY TO PRIVACY POLICY.—Paragraph (4) does not apply with respect to a privacy policy.

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

SEC. 209. PROHIBITION ON "DARK PATTERNS" IN NOTICE AND CONSENT PROCESSES AND PRIVACY POLICIES.

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

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

(2) understand the process for granting such consent;

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

(4) act on any such decision.

SEC. 210. NOTICE AND CONSENT REQUIRED.

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

(b) CONSENT.—

(1) EXPRESS CONSENT REQUIRED.—Except as provided in paragraphs (2) and (3), a covered entity may not collect from an individual personal information that creates or increases the risk of foreseeable privacy harms, or process or maintain any such personal information collected from an individual, unless such entity obtains the express consent of such individual to the collecting, processing, or maintaining (or any combination thereof) of such information through a process that is concise and clear and can

be objectively shown to meet the threshold established by the Director under section 208(a).

(2) EXCEPTION FOR IMPLIED CONSENT.—Notwithstanding paragraph (1), express consent is not required for collecting, processing, or maintaining personal information if the collecting, processing, or maintaining is, on its face, obvious and necessary to provide a service at the request of the individual and the personal information is collected, processed, or maintained only for such request. Nothing in this paragraph shall be construed to exempt the covered entity from the requirement of subsection (a) to provide notice to such individual with respect to such collecting, processing, or maintaining.

(3) EXEMPTION FOR PRIVACY-PRESERVING COMPUTING.—Notwithstanding paragraph (1), except with regard to consent for purposes of section 106, express consent is not required for collecting, processing, or maintaining personal information secured using privacy-preserving computing. Nothing in this paragraph shall be construed to exempt the covered entity from the requirement of subsection (a) to provide notice to such individual with respect to such collecting, processing, or maintaining.

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

SEC. 211. PRIVACY POLICY.

(a) POLICY REQUIRED.—A covered entity shall maintain a privacy policy relating to the practices of such entity regarding the collecting, processing, maintaining, and disclosing of personal information.

(b) CONTENTS.—The privacy policy required by subsection (a) shall contain the following:

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

(2) A description of how individuals may exercise the rights provided by title I.

(3) A clear and concise summary of the following:

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

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

(C) The categories and a list of third parties to which the covered entity discloses personal information.

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

(5) A list of the third parties to which the covered entity has disclosed personal information.

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

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

(c) EXEMPTION FOR PERSONAL INFORMATION FOR PARTICULAR PURPOSES.—The privacy policy required by subsection (a) is not required to contain information relating to personal information that is collected, processed, maintained, or disclosed exclusively for any of the purposes described in paragraph (1) of section 109(a) (or a combination of such purposes), except as provided in paragraph (2) of such section.

(d) AVAILABILITY OF PRIVACY POLICY.—

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

(A) clear and in plain language; and

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

(2) TIMING.—The privacy policy required by subsection (a) shall be made available as required by paragraph (1) before the covered entity collects personal information after the effective date of this Act.

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

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

SEC. 212. INFORMATION SECURITY REQUIREMENTS.

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

(1) the nature, scope, and complexity of the activities engaged in by such covered entity;

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

(3) the current state of the art in administrative, technical, and physical safeguards for protecting such information; and

(4) the cost of implementing such administrative, technical, and physical safeguards.

(b) SPECIFIC POLICIES, PRACTICES, AND PROCEDURES.—The policies, practices, and procedures required by subsection (a) shall include the following:

(1) A written security policy with respect to collecting, processing, maintaining, and disclosing of personal information. Such policy shall be made publicly available in a prominent location on an ongoing basis, except that the publicly available version is not required to contain information that would compromise a purpose described in section 109(a)(1).

(2) A process for identifying and assessing reasonably foreseeable security vulnerabilities in the system or systems used by such covered entity that contain personal information, which shall include regular monitoring for vulnerabilities or data breaches involving such system or systems.

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

process required by paragraph (2), which may include implementing any changes to security practices and the architecture, installation, or implementation of network or operating software, or for regularly testing or otherwise monitoring the effectiveness of the existing safeguards.

(4) A process for determining if personal information is no longer needed and disposing of personal information by shredding, permanently erasing, or otherwise modifying the medium on which such personal information is maintained to make such personal information permanently unreadable or indecipherable.

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

(6) A process for employee training and supervision for implementation of the policies, practices, and procedures required by this section.

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

(c) REGULATIONS.—The Director, in consultation with the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Tech-

nology, shall promulgate regulations to implement this section.

(d) SMALL BUSINESSES ASSISTANCE.—The Director, in consultation with the Cybersecurity and Infrastructure Security Agency, the National Institute of Standards and Technology, the Small Business Administration, the Minority Business Development Agency, and small businesses, shall develop policy templates, toolkits, tip sheets, configuration guidelines for commonly used hardware and software, interactive tools, and other materials to assist small businesses with complying with this section.

SEC. 213. NOTIFICATION OF DATA BREACH OR DATA-SHARING ABUSE.

(a) NOTIFICATION OF AGENCY.—

(1) IN GENERAL.—In the case of a data breach or data-sharing abuse with respect to personal information maintained by a covered entity, such covered entity shall, without undue delay and, if feasible, not later than 72 hours after becoming aware of such data breach or data-sharing abuse, notify the Director of such data breach or data-sharing abuse, unless such data breach or data-sharing abuse is unlikely to create or increase foreseeable privacy harms.

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

(b) NOTIFICATION OF OTHER COVERED ENTITY.—In the case of a data breach or data-sharing abuse with respect to personal information maintained by a covered entity that such covered entity obtained from another covered entity, the covered entity experiencing such data breach or data-sharing abuse shall, without undue delay and, if feasible, not later than 72 hours after becoming aware of such data breach or data-sharing abuse, notify such other covered entity of such data breach or data-sharing abuse, unless such data breach or data-sharing abuse is unlikely to create or increase foreseeable privacy harms. A covered entity receiving notice under this subsection of a data breach or data-sharing abuse shall notify any other covered entity from which the covered entity receiving notice obtained personal information involved in such data breach or data-sharing abuse, in the same manner as required under the preceding sentence for the covered entity experiencing such data breach or data-sharing abuse.

(c) NOTIFICATION OF INDIVIDUALS.—

(1) IN GENERAL.—In the case of a data breach or data-sharing abuse with respect to personal information maintained by a covered entity (or a data breach or data-sharing abuse about which a covered entity is notified under subsection (b)), if such covered entity has a relationship with an individual whose personal information was involved or potentially involved in such data breach or data-sharing abuse, such covered entity shall notify such individual of such data breach or data-sharing abuse not later than 14 days after becoming aware of such data breach or data-sharing abuse (or, in the case of a data breach or data-sharing abuse about which a covered entity is notified under subsection (b), not later than 14 days after being so notified), if such data breach or data-sharing abuse creates or increases foreseeable privacy harms.

(2) MEDIUM OF NOTIFICATION.—A covered entity shall notify an individual as required by paragraph (1) through—

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

(B) one additional medium of notification, if such covered entity has the personal information necessary to make a notification through such an additional medium without causing excessive financial burden for such covered entity.

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

TITLE III—DIGITAL PRIVACY AGENCY

SEC. 301. ESTABLISHMENT; DIRECTOR AND DEPUTY DIRECTOR.

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

(b) DIRECTOR.—

(1) IN GENERAL.—There is established the position of the Director, who shall serve as the head of the Agency.

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

(3) QUALIFICATION.—The President shall nominate the Director who, by reason of professional background and experience, is especially qualified to lead the Agency based on their knowledge and expertise in—

(A) privacy;

(B) information security;

(C) technology; and

(D) civil rights and civil liberties.

(4) TERM.—

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

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

(5) COMPENSATION.—

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

(B) CONFORMING AMENDMENT.—Section 5313 of title 5, United States Code, is amended by inserting after the item relating to the ''Chief Executive Officer, United States Inter-

national Development Finance Corporation.'' the following new item: ''Director of the Digital Privacy Agency.''.

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

(1) be appointed by the Director; and

(2) serve as acting Director in the absence or unavailability of the Director, notwithstanding section 3345 of title 5, United States Code.

(d) SERVICE RESTRICTION.—No Director or Deputy Director may hold any office, position, or employment in any covered entity during the period of service of such person as Director or Deputy Director.

(e) OFFICES.—The Director shall establish a principal office and field offices of the Agency in locations that have high levels of activity by covered entities, as determined by the Director.

SEC. 302. AGENCY POWERS AND AUTHORITIES.

(a) POWERS OF THE AGENCY.—The Director is authorized to establish the general policies of the Agency with respect to all executive and administrative functions, including—

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

(2) binding the Agency and enter into contracts;

(3) directing the establishment and continued operation of divisions or other offices within the Agency, in order to carry out the responsibilities of the Agency under this Act, and to satisfy the requirements of other applicable law;

(4) coordinating and overseeing the operation of all administrative, enforcement, and research activities of the Agency;

(5) adopting and using a seal;

(6) determining the character of and the necessity for the obligations and expenditures of the Agency;

(7) appointing and supervising of personnel employed by the Agency;

(8) distributing business among personnel appointed and supervised by the Director and among administrative units of the Agency;

(9) using and expending of funds;

(10) implementing this Act through rules, orders, guidance, interpretations, statements of policy, investigations, and enforcement actions; and

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

(b) DELEGATION OF AUTHORITY.—The Director may delegate to any duly authorized employee, representative, or agent any power vested in the Director or the Agency by law, except that the Director may not delegate the power to appoint the Deputy Director under section 301(c).

(c) AUTONOMY OF AGENCY REGARDING RECOMMENDATIONS AND TESTIMONY.—No officer or agency of the United States shall have any authority to require the Director or any other officer of the Agency to submit legislative recommendations, or testimony or comments on legislation, to any officer or agency of the United States for approval, comments, or review prior to the submission of such recommendations, testimony, or comments to the Congress, if such recommendations, testimony, or comments to the Congress include a statement indicating that the views expressed therein are those of the Director or such officer, and do not necessarily reflect the views of the President.

(d) RULEMAKING AUTHORITY.—

(1) IN GENERAL.—The Director may prescribe rules and issue orders and guidance, as may be necessary or appropriate to enable the Agency to implement, administer, and carry out the purposes and

objectives of this Act, and to prevent evasions thereof.

(2) REGULATIONS.—The Agency may issue regulations after notice and comment in accordance with section 553 of title 5, United States Code, as may be necessary to implement, administer, and carry out this Act.

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

(1) Federal agencies that have—

(A) jurisdiction over Federal privacy laws; and

(B) expertise in privacy or information security;

(2) State attorneys general, State privacy regulators, and other State agencies that have expertise in privacy or information security;

(3) international and intergovernmental bodies that conduct activities relating to the privacy or information security;

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

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

(6) advisory boards of the Agency established under section 308, as appropriate.

SEC. 303. REPORTING AND AUDIT REQUIREMENTS.

(a) REPORTS REQUIRED.—

(1) IN GENERAL.—Not later than 6 months after the date of the enactment of this Act, and every 6 months thereafter, the Director shall submit a report to the President and to the Committee on Energy and Commerce, the Committee on the Judiciary, and the Committee on Appropriations of the House of Representatives and the Committee on Commerce, Science, and Transportation, the Committee on the Judiciary, and the Committee on Appropriations of the Senate, and shall publish such report on the website of the Agency.

(2) CONTENTS.—Each report required by subsection (a) shall include—

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

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

(C) a list of the significant rules and orders adopted by the Agency, as well as other significant initiatives conducted by the Agency, during the preceding 6-month period and the plan of the Agency for rules, orders, or other initiatives to be undertaken during the upcoming 6-month period;

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

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

(F) an assessment of significant actions by State attorneys general or State privacy regulators relating to this Act or the rules prescribed under this Act during the preceding 6-month period.

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

SEC. 304. RELATION TO OTHER AGENCIES.

(a) COORDINATION.—

(1) IN GENERAL.—With respect to covered entities and service providers, to the extent that Federal law authorizes the Agency and another Federal agency to enforce a Federal privacy law, the other Federal agency shall coordinate with the Agency to promote consistent enforcement of this Act and the other Federal privacy law.

(2) REFERRAL.—Any Federal agency authorized to enforce Federal privacy laws may recommend in writing to the Agency that the Agency initiate an enforcement proceeding, as the Agency is authorized by that Federal privacy law or by this Act.

(b) TRANSFERS FROM THE COMMISSION.—

(1) TRANSFERS OF AUTHORITY.—

(A) TRANSFER OF RULEMAKING AND CERTAIN OTHER AUTHORITIES UNDER FEDERAL PRIVACY LAWS.—The Agency shall have all powers and duties under the Federal privacy laws to prescribe rules, issue guidelines, or to conduct studies or issue reports mandated by such laws, that were vested in the Commission on the effective date of this Act. The authority of the Commission under Federal privacy laws to prescribe rules, issue guidelines, or conduct

a study or issue a report mandated under such law shall be transferred to the Agency on the effective date of this Act.

(B) TRANSFER OF ENFORCEMENT AUTHORITY.—The Agency may enforce a rule prescribed by the Commission under—

(i) Federal privacy laws; or

(ii) the Federal Trade Commission Act (15 U.S.C. 41 et seq.) related to unfair or deceptive acts or practices relating to privacy, information security, identity theft, data abuses, and related matters.

(2) TRANSFER OF PRIVACY EMPLOYEES.—Any employee of the Commission employed in a division, bureau, office, or other subdivision of the Commission with the primary responsibility of administering, investigating, or enforcing Federal privacy laws or applications of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) related to unfair or deceptive acts or practices relating to privacy, information security, identity theft, data abuses, and related matters shall be transferred to the Agency. Such employee shall be provided with compensation and benefits not less than the equivalent of compensation and benefits provided to such employee on

the date of enactment of this Act or compensation and benefits provided to an employee of the Agency in comparable position with comparable experience.

(c) PRESERVATION OF AUTHORITIES OF OTHER AGENCIES.—Except as described in this section, no provision of this Act shall be construed as modifying, limiting, or otherwise affecting the operation of any provision of Federal law, or otherwise affecting the authority of any Federal agency under a Federal privacy law or any other law, including the ability of such Federal agency to promulgate regulations and enforce Federal privacy laws.

SEC. 305. PERSONNEL.

(a) PERSONNEL.—

(1) APPOINTMENT GENERALLY.—The Director may fix the number of, and appoint and direct, all employees of the Agency, in accordance with the applicable provisions of title 5, United States Code. The Director may appoint personnel without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, so long as the Director sets requirements, conducts recruitment, and determines appointments in a fair, transparent, and equitable manner.

(2) EMPLOYEES OF THE AGENCY.—The Director is authorized to employ privacy experts, tech-

nologists, computer scientists, user experience designers and researchers, data scientists, ethicists, attorneys, investigators, economists, civil rights experts, and other employees as the Director considers necessary to conduct the business of the Agency. Unless otherwise provided expressly by law, any individual appointed under this section shall be an employee, as defined in section 2105 of title 5, United States Code, and subject to the provisions of such title and other laws generally applicable to the employees of an executive agency.

(3) EMPLOYEE COMPENSATION.—The Director may fix and adjust the pay and benefits of personnel as the Director considers desirable, competitive, transparent, and equitable, without regard to the provisions of chapter 51 and subchapter III of chapter 53 of title 5, United States Code, relating to classification and General Schedule pay rates, respectively.

(4) LABOR-MANAGEMENT RELATIONS.—Chapter 71 of title 5, United States Code, shall apply to the Agency and the employees of the Agency.

(b) ADDITIONAL ROLES.—

(1) CHIEF INFORMATION OFFICER.—

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

(i) in section 11315(c) by adding ''and of the Digital Privacy Agency'' before the em dash immediately preceding paragraph (1); and

(ii) in section 11319(a)(1) by adding ''and the Digital Privacy Agency'' before the period.

(B) RESPONSIBILITY.—The Chief Information Officer of the Digital Privacy Agency, as designated by subparagraph (A), shall ensure the Digital Privacy Agency uses technology efficiency to implement, administer, and enforce this Act and the rules and orders issued pursuant to this Act.

(2) INSPECTOR GENERAL.—Section 12 of the Inspector General Act of 1978 (5 U.S.C. App.) is amended—

(A) in paragraph (1), by inserting ''the Director of the Digital Privacy Agency;'' after ''the President of the Export-Import Bank;''; and

(B) in paragraph (2), by inserting ''the Digital Privacy Agency,'' after ''the Export-Import Bank,''.

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

(A) act as a liaison between the Agency and any affected person with respect to any problem that such person may have in dealing with the Agency that results from the regulatory activities of the Agency; and

(B) assure that safeguards exist to encourage complainants to come forward and preserve confidentiality.

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

SEC. 306. OFFICE OF CIVIL RIGHTS.

The Director shall establish an Office of Civil Rights within the Agency that shall have following responsibilities:

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

(2) Developing, establishing, and promoting practices that affirmatively further equal opportunity to and expand access to employment (including hiring, firing, promotion, demotion, and compensation), credit and insurance (including denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services.

(3) Coordinating the Agency's civil rights efforts with other Federal agencies and State regulators, as appropriate, to promote consistent, efficient, and effective enforcement of Federal civil rights laws.

(4) Working with civil rights advocates, privacy experts, and other experts (including members of the advisory boards established under section 308) on the promotion of compliance with the civil rights

provisions under this Act, rules and orders issued pursuant this Act, and Federal privacy laws.

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

(6) Providing annual reports to Congress on the efforts of the Agency to fulfill its civil rights mandate.

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

SEC. 307. COMPLAINTS OF INDIVIDUALS.

(a) IN GENERAL.—The Director shall establish a unit within the Agency the functions of which shall include establishing a single, toll-free telephone number, a website, and a database or utilizing an existing database to facilitate the centralized collection of, monitoring of, and response to complaints of individuals regarding the privacy or security of personal information. The Director shall coordinate with other Federal agencies with jurisdiction over Federal privacy laws to route complaints to such agencies, where appropriate.

(b) ROUTING COMPLAINTS TO STATES.—To the extent practicable, State agencies (including State privacy

regulators) may receive appropriate complaints from the systems established under subsection (a), if—

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

(2) the State agency has satisfied any conditions of participation in the system that the Agency may establish, including treatment of personal information and sharing of information on complaint resolution or related compliance procedures and resources; and

(3) participation by the State agency includes measures necessary to provide for protection of personal information that conform to the standards for protection of the confidentiality of personal information and for data integrity and security that apply to Federal agencies.

(c) DATA SHARING REQUIRED.—To facilitate inclusion in the reports required by section 303 of the matters regarding complaints of individuals required by subsection (a)(2)(D) of such section to be included in such reports, investigation and enforcement activities, and monitoring of the privacy and security of personal information, the Agency shall share information about complaints of individuals with Federal and State agencies (including State

privacy regulators) that have jurisdiction over the privacy or security of personal information and State attorneys general, subject to the standards applicable to Federal agencies for the protection of the confidentiality of personal information and for information security and integrity. Other Federal agencies that have jurisdiction over the privacy or security of personal information shall share data relating to complaints of individuals regarding the privacy or security of personal information with the Agency, subject to the standards applicable to Federal agencies for the protection of confidentiality of personal information and for information security and integrity.

(d) PUBLISHING OF COMPLAINTS.—

(1) CONSENT REQUIRED.—In collecting a complaint from an individual, the Agency shall request consent for publishing the complaint without any information identifying the individual.

(2) PUBLIC DATABASE.—The Agency shall make publicly available on its website a database of each complaint for which it has received consent to publish the complaint from an individual who provided the complaint to the Agency.

(3) REDACTING INFORMATION.—When necessary, the Agency may redact information from a

published complaint to protect the privacy of the individual.

SEC. 308. ADVISORY BOARDS.

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

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

(2) The Research Advisory Board, which shall be composed of individuals with academic and research expertise in privacy, cybersecurity, computer science, innovation, design, ethics, economics, law, and public policy.

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

(4) The Product Advisory Board, which shall be composed of technologists, computer scientists, designers, product managers, attorneys, and other representatives of covered entities.

(b) APPOINTMENTS.—The Director shall appoint members to the advisory boards established under subsection (a) without regard to party affiliation.

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

(d) COMPENSATION AND TRAVEL EXPENSES.—Members of the advisory boards established under subsection (a) who are not full-time employees of the United States shall—

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

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

SEC. 309. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Director to carry out this Act $550,000,000 for each of the fiscal years 2024, 2025, 2026, 2027, and 2028.

TITLE IV—ENFORCEMENT

SEC. 401. INVESTIGATIONS AND ADMINISTRATIVE DISCOVERY.

(a) JOINT INVESTIGATIONS.—The Agency or, where appropriate, an Agency investigator, may conduct investigations and make requests for information, as authorized under this Act, on a joint basis with another Federal agency, a State attorney general, or a State privacy regulator.

(b) SUBPOENAS.—

(1) IN GENERAL.—The Agency or an Agency investigator may issue subpoenas for the attendance and testimony of witnesses and the production of relevant papers, books, documents, or other material in connection with hearings under this Act.

(2) FAILURE TO OBEY.—In the case of contumacy or refusal to obey a subpoena issued pursuant to this subsection and served upon any person, the district court of the United States for any district in which such person is found, resides, or transacts business, upon application by the Agency or an Agency investigator and after notice to such person, may issue an order requiring such person to appear and give testimony or to appear and produce documents or other material.

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

(c) DEMANDS.—

(1) IN GENERAL.—Whenever the Agency has reason to believe that any person may be in possession, custody, or control of any documentary material or tangible things, or may have any information, relevant to a violation, the Agency may, before the institution of any proceedings under this Act, issue in writing, and cause to be served upon such person, a civil investigative demand requiring such person to—

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

(B) submit such tangible things;

(C) file written reports or answers to questions;

(D) give oral testimony concerning documentary material, tangible things, or other information; or

(E) furnish any combination of such material, answers, or testimony.

(2) REQUIREMENTS.—Each civil investigative demand shall state the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable to such violation.

(3) PRODUCTION OF DOCUMENTS.—Each civil investigative demand for the production of documentary material shall—

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

(B) prescribe a return date or dates which will provide a reasonable period of time within which the material so demanded may be assembled and made available for inspection and copying or reproduction; and

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

(4) PRODUCTION OF THINGS.—Each civil investigative demand for the submission of tangible things shall—

(A) describe each class of tangible things to be submitted under the demand with such

definiteness and certainty as to permit such things to be fairly identified;

(B) prescribe a return date or dates which will provide a reasonable period of time within which the things so demanded may be assembled and submitted; and

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

(5) DEMAND FOR WRITTEN REPORTS OR ANSWERS.—Each civil investigative demand for written reports or answers to questions shall—

(A) propound with definiteness and certainty the reports to be produced or the questions to be answered;

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

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

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

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

(B) identify an Agency investigator who shall conduct the investigation and the custo-

dian to whom the transcript of such investigation shall be submitted.

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

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

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

(i) in such manner as the Federal Rules of Civil Procedure prescribe for service in a foreign nation; and

(ii) to the extent that the courts of the United States have authority to assert jurisdiction over such person, consistent with due process, the United States District Court for the District of Columbia shall have the same jurisdiction to take any action respecting compliance with this section by such person that such district court would have if such person were personally within the jurisdiction of such district court.

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

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

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

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

(9) PROOF OF SERVICE.—

(A) IN GENERAL.—A verified return by the individual serving any civil investigative demand or any enforcement petition filed under this section setting forth the manner of such service shall be proof of such service.

(B) RETURN RECEIPTS.—In the case of service by registered or certified mail, such return shall be accompanied by the return post office receipt of delivery of such demand or enforcement petition.

(10) PRODUCTION OF DOCUMENTARY MATERIAL.—The production of documentary material in response to a civil investigative demand shall be made under a sworn certificate, in such form as the demand designates, by the person, if a natural person, to whom the demand is directed or, if not a natural person, by any person having knowledge of the facts and circumstances relating to such production, to the effect that all of the documentary material required by the demand and in the possession, custody, or control of the person to whom the demand is directed has been produced and made available to the custodian.

(11) SUBMISSION OF TANGIBLE THINGS.—The submission of tangible things in response to a civil investigative demand shall be made under a sworn certificate, in such form as the demand designates, by the person to whom the demand is directed or, if not a natural person, by any person having knowledge of the facts and circumstances relating to such

production, to the effect that all of the tangible things required by the demand and in the possession, custody, or control of the person to whom the demand is directed have been submitted to the custodian.

(12) SEPARATE ANSWERS.—Each reporting requirement or question in a civil investigative demand shall be answered separately and fully in writing under oath, unless it is objected to, in which event the reasons for the objection shall be stated in lieu of an answer, and it shall be submitted under a sworn certificate, in such form as the demand designates, by the person, if a natural person, to whom the demand is directed or, if not a natural person, by any person responsible for answering each reporting requirement or question, to the effect that all information required by the demand and in the possession, custody, control, or knowledge of the person to whom the demand is directed has been submitted.

(13) TESTIMONY.—

(A) IN GENERAL.—

(i) OATH AND RECORDATION.—The examination of any person pursuant to a demand for oral testimony served under this subsection shall be taken before an of-

ficer authorized to administer oaths and affirmations by the laws of the United States or of the place at which the examination is held. The officer before whom oral testimony is to be taken shall put the witness on oath or affirmation and shall personally, or by any individual acting under the direction of and in the presence of the officer, record the testimony of the witness.

(ii) TRANSCRIPTION.—The testimony shall be taken stenographically and transcribed.

(B) PARTIES PRESENT.—Any Agency investigator before whom oral testimony is to be taken shall exclude from the place where the testimony is to be taken all other persons, except the person giving the testimony, the attorney for that person, the officer before whom the testimony is to be taken, an investigator or representative of an agency with which the Agency is engaged in a joint investigation, and any stenographer taking such testimony.

(C) LOCATION.—The oral testimony of any person taken pursuant to a civil investigative

demand shall be taken in the judicial district of the United States in which such person resides, is found, or transacts business, or in such other place as may be agreed upon by the Agency investigator before whom the oral testimony of such person is to be taken and such person.

(D) ATTORNEY REPRESENTATION.—

(i) IN GENERAL.—Any person compelled to appear under a civil investigative demand for oral testimony pursuant to this subsection may be accompanied, represented, and advised by an attorney.

(ii) AUTHORITY.—The attorney may advise a person described in clause (i), in confidence, either upon the request of such person or upon the initiative of the attorney, with respect to any question asked of such person.

(iii) OBJECTIONS.—A person described in clause (i), or the attorney for that person, may object on the record to any question, in whole or in part, and such person shall briefly state for the record the reason for the objection. An objection may properly be made, received, and entered

upon the record when it is claimed that such person is entitled to refuse to answer the question on grounds of any constitutional or other legal right or privilege, including the privilege against self-incrimination, but such person shall not otherwise object to or refuse to answer any question, and such person or attorney shall not otherwise interrupt the oral examination.

(iv) REFUSAL TO ANSWER.—If a person described in clause (i) refuses to answer any question—

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

(II) if the refusal is on grounds of the privilege against self-incrimination, the testimony of such person may be compelled in accordance with the provisions of section 6004 of title 18, United States Code.

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

(i) after the testimony of any witness is fully transcribed, the Agency investigator shall afford the witness (who may be accompanied by an attorney) a reasonable opportunity to examine the transcript;

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

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

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

(v) if the transcript is not signed by the witness during the 30-day period following the date on which the witness is first afforded a reasonable opportunity to examine the transcript, the Agency investigator shall sign the transcript and state on the record the fact of the waiver, illness,

absence of the witness, or the refusal to sign, together with any reasons given for the failure to sign.

(F) CERTIFICATION BY INVESTIGATOR.—The Agency investigator shall certify on the transcript that the witness was duly sworn by such Agency investigator and that the transcript is a true record of the testimony given by the witness, and the Agency investigator shall promptly deliver the transcript or send it by registered or certified mail to the custodian.

(G) COPY OF TRANSCRIPT.—The Agency investigator shall furnish a copy of the transcript (upon payment of reasonable charges for the transcript) to the witness only, except that the Agency may for good cause limit such witness to inspection of the official transcript of the testimony of such witness.

(H) WITNESS FEES.—Any witness appearing for the taking of oral testimony pursuant to a civil investigative demand shall be entitled to the same fees and mileage which are paid to witnesses in the district courts of the United States.

(d) CONFIDENTIAL TREATMENT OF DEMAND MATERIAL.—

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

(2) DISCLOSURE TO CONGRESS.—No rule established by the Agency regarding the confidentiality of materials submitted to, or otherwise obtained by, the Agency shall be intended to prevent disclosure to either House of Congress or to an appropriate committee of the Congress, except that the Agency is permitted to adopt rules allowing prior notice to any party that owns or otherwise provided the material to the Agency and had designated such material as confidential.

(e) PETITION FOR ENFORCEMENT.—

(1) IN GENERAL.—Whenever any person fails to comply with any civil investigative demand duly served upon such person under this section, or whenever satisfactory copying or reproduction of material requested pursuant to the demand cannot be accomplished and such person refuses to surrender such material, the Agency, through such officers or attor-

neys as it may designate, may file, in the district court of the United States for any judicial district in which such person resides, is found, or transacts business, and serve upon such person, a petition for an order of such court for the enforcement of this section.

(2) SERVICE OF PROCESS.—All process of any court to which application may be made as provided in this subsection may be served in any judicial district.

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

(1) IN GENERAL.—Not later than 20 days after the service of any civil investigative demand upon any person under subsection (c), or at any time before the return date specified in the demand, whichever period is shorter, or within such period exceeding 20 days after service or in excess of such return date as may be prescribed in writing, subsequent to service, by any Agency investigator named in the demand, such person may file with the Agency a petition for an order by the Agency modifying or setting aside the demand.

(2) COMPLIANCE DURING PENDENCY.—The time permitted for compliance with the demand in

whole or in part, as determined proper and ordered by the Agency, shall not run during the pendency of a petition under paragraph (1) at the Agency, except that such person shall comply with any portions of the demand not sought to be modified or set aside.

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

(g) CUSTODIAL CONTROL.—At any time during which any custodian is in custody or control of any documentary material, tangible things, reports, answers to questions, or transcripts of oral testimony given by any person in compliance with any civil investigative demand, such person may file, in the district court of the United States for the judicial district within which the office of such custodian is situated, and serve upon such custodian, a petition for an order of such court requiring the performance by such custodian of any duty imposed upon such custodian by this section or rule promulgated by the Agency.

(h) JURISDICTION OF COURT.—

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

(2) APPEAL.—Any final order entered as described in paragraph (1) shall be subject to appeal pursuant to section 1291 of title 28, United States Code.

SEC. 402. HEARINGS AND ADJUDICATION PROCEEDINGS.

(a) IN GENERAL.—The Agency is authorized to conduct hearings and adjudication proceedings with respect to any person in the manner prescribed by chapter 5 of title 5, United States Code, in order to ensure or enforce compliance with this Act and the rules prescribed under this Act.

(b) SPECIAL RULES FOR CEASE-AND-DESIST PROCEEDINGS.—

(1) ORDERS AUTHORIZED.—

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

Act, the Agency may issue and serve upon the person a notice of charges in respect thereof.

(B) CONTENT OF NOTICE.—The notice under subparagraph (A) shall contain a statement of the facts constituting the alleged violation, and shall fix a time and place at which a hearing will be held to determine whether an order to cease and desist should issue against the person, such hearing to be held not earlier than 30 days nor later than 60 days after the date of service of such notice, unless an earlier or a later date is set by the Agency, at the request of any person so served.

(C) CONSENT.—Unless a person served under subparagraph (B) appears at the hearing personally or by a duly authorized representative, the person shall be deemed to have consented to the issuance of the cease-and-desist order.

(D) PROCEDURE.—In the event of consent under subparagraph (C), or if, upon the record made at any such hearing, the Agency finds that any violation specified in the notice of charges has been established, the Agency may issue and serve upon the person an order to

cease and desist from the violation. Such order may, by provisions which may be mandatory or otherwise, require the person to cease and desist from the subject act or omission, and to take affirmative action to correct the conditions resulting from any such violation.

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

(3) DECISION AND APPEAL.—Any hearing provided for in this subsection shall be held in the Federal judicial district or in the territory in which the residence or principal office or place of business of the person is located unless the person consents to another place, and shall be conducted in accordance with the provisions of chapter 5 of title 5, United States Code. After such hearing, and not later than 90 days after the Agency has notified each party to

the proceeding that the case has been submitted to the Agency for final decision, the Agency shall render its decision (which shall include findings of fact upon which its decision is predicated) and shall issue and serve upon each such party an order or orders consistent with the provisions of this section. Judicial review of any such order shall be exclusively as provided in this subsection. Unless a petition for review is timely filed in a court of appeals of the United States, as provided in paragraph (4), and thereafter until the record in the proceeding has been filed as provided in paragraph (4), the Agency may at any time, upon such notice and in such manner as the Agency shall determine proper, modify, terminate, or set aside any such order. Upon filing of the record as provided, the Agency may modify, terminate, or set aside any such order with permission of the court.

(4) APPEAL TO COURT OF APPEALS.—Any party to any proceeding under this subsection may obtain a review of any order served pursuant to this subsection (other than an order issued with the consent of the party) by filing in the court of appeals of the United States for the circuit in which the residence or principal office or place of business of the

party is located, or in the United States Court of Appeals for the District of Columbia Circuit, within 30 days after the date of service of such order, a written petition praying that the order of the Agency be modified, terminated, or set aside. A copy of such petition shall be forthwith transmitted by the clerk of the court to the Agency, and thereupon the Agency shall file in the court the record in the proceeding, as provided in section 2112 of title 28, United States Code. Upon the filing of such petition, such court shall have jurisdiction, which upon the filing of the record shall, except as provided in the last sentence of paragraph (3), be exclusive, to affirm, modify, terminate, or set aside, in whole or in part, the order of the Agency. Review of such proceedings shall be had as provided in chapter 7 of title 5, United States Code. The judgment and decree of the court shall be final, except that the same shall be subject to review by the Supreme Court of the United States, upon certiorari, as provided in section 1254 of title 28, United States Code.

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

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

(1) IN GENERAL.—Whenever the Agency determines that the violation specified in the notice of charges served upon a person pursuant to subsection (b), or the continuation thereof, is likely to cause the person to be insolvent or otherwise prejudice the interests of individuals before the completion of the proceedings conducted pursuant to subsection (b), the Agency may issue a temporary order requiring the person to cease and desist from any such violation and to take affirmative action to prevent or remedy such insolvency or other condition pending completion of such proceedings. Such order may include any requirement authorized under this title. Such order shall become effective upon service upon the person and, unless set aside, limited, or suspended by a court in proceedings authorized by paragraph (2), shall remain effective and enforceable pending the completion of the administrative proceedings pursuant to such notice and until such time as the Agency shall dismiss the charges specified in such notice, or if a cease-and-desist order is issued against the person, until the effective date of such order.

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

(d) SPECIAL RULES FOR ENFORCEMENT OF ORDERS.—

(1) IN GENERAL.—The Agency may in its discretion apply to the United States district court within the jurisdiction of which the residence or principal office or place of business of a person is located, for the enforcement of any effective and outstanding order issued under this section against such person, and such court shall have jurisdiction and power to order and require compliance with such order.

(2) EXCEPTION.—Except as otherwise provided in this section, no court shall have jurisdiction to affect by injunction or otherwise the issuance or enforcement of any order or to review, modify, suspend, terminate, or set aside any such order.

(e) RULES.—The Agency shall prescribe rules establishing such procedures as may be necessary to carry out this section.

SEC. 403. LITIGATION AUTHORITY.

(a) IN GENERAL.—If a person violates any provision of this Act or a rule or order prescribed under this Act, the Agency may commence a civil action against such person to impose a civil penalty or to seek all appropriate legal and equitable relief, including a permanent or temporary injunction as permitted by law.

(b) REPRESENTATION.—Except as provided in subsection (e), the Agency may act in its own name and through its own attorneys enforcing any provision of this Act or rules or orders issued pursuant to this Act or in any action, suit, or other court proceeding to which the Agency is a party.

(c) COMPROMISE OF ACTIONS.—The Agency may compromise or settle any action, suit, or other court proceeding to which the Agency is a party if such compromise is approved by the court.

(d) NOTICE TO THE ATTORNEY GENERAL OF THE UNITED STATES.—

(1) IN GENERAL.—When commencing a civil action under this Act or regulations or rules or orders issued pursuant to this Act, the Agency shall notify the Attorney General.

(2) NOTICE AND COORDINATION.—

(A) NOTICE OF OTHER ACTIONS.—In addition to any notice required under paragraph (1), the Agency shall notify the Attorney General concerning any action, suit, or other court proceeding to which the Agency is a party.

(B) COORDINATION.—In order to avoid conflicts and promote consistency regarding litigation of matters under Federal law, the Attorney General and the Agency shall consult regarding the coordination of investigations and proceedings, including by negotiating an agreement for coordination not later than 180 days after the effective date of this Act. The agreement under this subparagraph shall include provisions to ensure that parallel investigations and proceedings involving this Act and the rules prescribed under this Act are conducted in a manner that avoids conflicts and does not im-

pede the ability of the Attorney General to prosecute violations of Federal criminal laws.

(C) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to limit the authority of the Agency under this Act, including the authority to interpret this Act.

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

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

(g) TIME FOR BRINGING ACTION.—Except as otherwise permitted by law or equity, no action may be brought under this Act more than 3 years after the date of discovery of the violation to which the action relates.

SEC. 404. ENFORCEMENT BY STATES.

(a) CIVIL ACTION.—In any case in which a State attorney general or a State privacy regulator has reason to believe that an interest of the residents of a State has been or is adversely affected by any person who violates any provision of this Act or a rule or order prescribed under this Act, the State attorney general or State privacy regulator, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate State court or an appropriate district court of the United States to—

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

(2) compel compliance with such provision; or

(3) obtain relief under section 406.

(b) RIGHTS OF AGENCY.—Before initiating a civil action under subsection (a), the State attorney general or State privacy regulator, as the case may be, shall notify the Agency in writing of such civil action. Upon receiving notice with respect to a civil action, the Agency may—

(1) intervene in such action; and

(2) upon intervening—

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

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

(c) PREEMPTIVE ACTION BY AGENCY.—If the Agency institutes a civil action for violation of any provision of this Act or a rule or order prescribed under this Act, no State attorney general or State privacy regulator may bring a civil action against any defendant named in the complaint of the Agency for a violation of such provision that is alleged in such complaint.

SEC. 405. PRIVATE RIGHTS OF ACTION.

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

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

(c) NONPROFIT COLLECTIVE REPRESENTATION.—An individual shall have the right to appoint a nonprofit organization (as described in section 501(c)(3) of the Internal Revenue Code of 1986 and exempt from taxation under section 501(a) of such Code) which has been properly constituted in accordance with the law, has statutory

objectives which are in the public interest, and is active in the field of the protection of individual rights and freedoms with regard to the protection of privacy and information security to lodge the complaint on behalf of such individual to exercise the rights referred to in this Act on behalf of such individual.

(1) A nonprofit may represent a class of aggrieved individuals.

(2) A prevailing nonprofit shall receive reasonable compensation for expenses, including attorneys' fees.

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

(d) STATE APPOINTMENT.—A State may provide that any body, organization, or association referred to in subsection (c), independent of an individual's appointment, has the right to lodge, in that State, a complaint with the Agency and to exercise the rights referred to in this Act if it considers that the rights of an individual under this Act have been infringed.

SEC. 406. RELIEF AVAILABLE.

(a) CIVIL ACTIONS AND ADJUDICATION PROCEEDINGS.—

(1) JURISDICTION.—In any civil action or any adjudication proceeding brought by the Agency, a

State attorney general, or State privacy regulator under any provision of this Act or a rule or order prescribed under this Act, the court or the Agency (as the case may be) shall have jurisdiction to grant any appropriate legal or equitable relief with respect to a violation of such provision.

(2) RELIEF.—Relief under this section may include—

(A) rescission or reformation of contracts;

(B) refund of moneys;

(C) restitution;

(D) disgorgement or compensation for unjust enrichment;

(E) payment of damages or other monetary relief;

(F) public notification regarding the violation, including the costs of notification;

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

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

(3) NO EXEMPLARY OR PUNITIVE DAMAGES.—Nothing in this subsection shall be construed as authorizing the imposition of exemplary or punitive damages.

(b) RECOVERY OF COSTS.—In any civil action brought by the Agency, State attorney general, or State privacy regulator under any provision of this Act or a rule or order prescribed under this Act, the Agency, State attorney general, or State privacy regulator may recover its costs in connection with prosecuting such action if the Agency or State attorney general is the prevailing party in the action.

(c) CIVIL MONEY PENALTY IN COURT AND ADMINISTRATIVE ACTIONS.—

(1) IN GENERAL.—Any person who violates, through any act or omission, any provision of this Act or a rule or order issued pursuant to this Act shall forfeit and pay a civil penalty under this subsection.

(2) PENALTY AMOUNT.—

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

(i) the maximum civil penalty for which a person, partnership, or corporation may be liable under section 5(m)(1)(A) of the Federal Trade Commission Act (15 U.S.C. 45(m)(1)(A)) for a violation of a rule under such Act respecting unfair or

deceptive acts or practices, as adjusted under the Federal Civil Penalties Inflation Adjustment Act of 1990 (28 U.S.C. 2461 note); and

(ii) the number of individuals whose personal information is affected by the violation.

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

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

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

(B) the gravity of the violation;

(C) the severity of the privacy harms (including both actual and potential harms) to individuals;

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

(E) the history of previous violations; and

(F) such other matters as justice may require.

(4) AUTHORITY TO MODIFY OR REMIT PENALTY.—The Agency, State attorney general, or State privacy regulator may compromise, modify, or remit any penalty which may be assessed or has already been assessed under paragraph (2). The amount of such penalty, when finally determined, shall be exclusive of any sums owed by the person to the United States in connection with the costs of the proceeding, and may be deducted from any sums owing by the United States to the person charged.

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

(A) the Agency, State attorney general, or State privacy regulator gives notice and an opportunity for a hearing to the person accused of the violation; or

(B) the appropriate court has ordered such assessment and entered judgment in favor of the Agency, State attorney general, or State privacy regulator.

SEC. 407. REFERRAL FOR CRIMINAL PROCEEDINGS.

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

SEC. 408. WHISTLEBLOWER ENFORCEMENT.

(a) IN GENERAL.—Any person who becomes aware, based on nonpublic information, that a covered entity has violated this Act may file a civil action for civil penalties, if prior to filing such action, the person files with the Director a written request for the Director to commence the action. The request shall include a clear and concise statement of the grounds for believing a cause of action exists. The person shall make the nonpublic information available to the Director upon request:

(1) If the Director files suit within 90 days from receipt of the written request to commence the action, no other action may be brought unless the

action brought by the Director is dismissed without prejudice.

(2) If the Director does not file suit within 90 days from receipt of the written request to commence the action, the person requesting the action may proceed to file a civil action.

(3) The time period within which a civil action shall be commenced shall be tolled from the date of receipt by the Director of the written request to either the date that the civil action is dismissed without prejudice, or for 150 days, whichever is later, but only for a civil action brought by the person who requested the Director to commence the action.

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

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

(2) If the action was brought by the person who made the request pursuant to subsection (a), that person shall receive an amount the court determines

is reasonable for collecting the civil penalties on behalf of the government. The amount shall be not less than 25 percent and not more than 50 percent of the proceeds of the action and shall be paid out of the proceeds.

TITLE V—RELATION TO OTHER LAW

SEC. 501. EFFECTIVE DATE.

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

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

SEC. 502. RELATION TO OTHER FEDERAL LAW.

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

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

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

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

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

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

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

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

(8) Section 444 of the General Education Provisions Act (20 U.S.C. 1232g) (commonly known as the ''Family Educational Rights and Privacy Act of 1974'').

(9) Section 445 of the General Education Provisions Act (20 U.S.C. 1232h).

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

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

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

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

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

(13) Section 222, 227, 338, or 631 of the Communications Act of 1934 (47 U.S.C. 222, 227, 338, or 551).

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

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

(16) The Federal Information Security Management Act of 2002 (44 U.S.C. 3541 et seq.).

(17) The Currency and Foreign Transactions Reporting Act of 1970, as amended (commonly known as the ''Bank Secrecy Act'') (12 U.S.C. 1829b and 1951–1959, 31 U.S.C. 5311–5314 and 5316–5332), including the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, title III of Public Law 107–56, as amended.

(18) The National Security Act of 1947 (50 U.S.C. 3001 et seq.).

(19) The Foreign Intelligence Surveillance Act of 1978, as amended (50 U.S.C. 1801 et seq.).

(20) The Civil Rights Act of 1964 (Public Law 88–352, 78 Stat. 241).

(21) The Americans with Disabilities Act (42 U.S.C. 12101 et seq.).

(22) The Fair Housing Act (42 U.S.C. 3601 et seq.).

(23) The Consumer Financial Protection Act of 2010 (12 U.S.C. 5481 et seq.).

(24) The Equal Credit Opportunity Act (15 U.S.C. 1691 et seq.).

(25) The Age Discrimination in Employment Act (29 U.S.C. 621 et seq.).

(26) The Genetic Information Nondiscrimination Act (Public Law 110–233, 122 Stat. 881).

(27) Subpart A of part 46 of title 45, Code of Federal Regulations (commonly known as the ''Common Rule'').

(28) The Driver's Privacy Protection Act of 1994 (18 U.S.C. 2721 et seq.).

(29) The Video Privacy Protection Act (18 U.S.C. 2710 et seq.).

(30) Chapters 61, 68, 75, and 76 of the Internal Revenue Code of 1986.

(31) Section 1106 of the Social Security Act (42 U.S.C. 1306).

(32) The Stored Communications Act (18 U.S.C. 2701 et seq.).

(33) Any other privacy or information security provision of Federal law.

SEC. 503. RELATION TO STATE LAW.

This Act, and any amendment, standard, rule, requirement, assessment, or regulation promulgated under this Act, does not annul, alter, affect, or exempt any person subject to the provisions of this Act from complying with the laws of any State or political subdivision of a State with respect to privacy or consumer protection, except to the extent that those laws are inconsistent with any provisions of this Act, and then only to the extent of the inconsistency. For purposes of this section, a law of a State or political subdivision of a State is not inconsistent with this Act if the protection such law affords any consumer is greater than the protection provided by this Act.

SEC. 504. SEVERABILITY.

If any provision of this Act or the amendments made by this Act, or the application thereof, is held unconstitutional or otherwise invalid, the validity of the remainder

of the Act, the amendments, and the application of such provision shall not be affected thereby.

TITLE VI—NIST AND NSF ACTIVITIES

SEC. 601. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY PRIVACY RESEARCH AND DEVELOPMENT.

Section 2 of the National Institute of Standards and Technology Act (15 U.S.C. 272) is amended by adding at the end the following:

''(f) PRIVACY RISK MANAGEMENT RESEARCH.—In carrying out the activities under subsection (c)(19), the Director shall, to the extent practicable and appropriate—

''(1) develop, and periodically update, in collaboration with appropriate Federal agencies, industry, State, local, and Tribal governments, civil society, other nonprofit organizations, and the Information Security and Privacy Advisory Board, a privacy risk management framework that covers risks associated with data processing and that shall—

''(A) identify voluntary, consensus-based technical standards, guidelines, best practices, methodologies, procedures, and processes for—

"(i) developing privacy-enhanced information systems and networks, including emerging technologies; and

"(ii) assessing and mitigating privacy risks to help organizations protect individuals' privacy in information systems and networks;

"(B) establish common definitions and characterizations for aspects of privacy risk management;

"(C) provide case studies and risk profiles of framework implementation;

"(D) provide guidance to enable organizations to use the framework to meet privacy requirements from Federal, State, local, and Tribal governments and international policymakers;

"(E) incorporate voluntary, consensus-based technical standards and best practices;

"(F) facilitate use by regulators and markets with the aim of reducing barriers to trade; and

"(G) not prescribe or otherwise require the use of specific information or communications technology products or services;

''(2) carry out research associated with mitigating privacy risks associated with information systems and networks, including to inform periodic updates to the privacy risk management framework developed pursuant to paragraph (1);

''(3) in consultation with the Director of the Digital Privacy Agency, the Federal Trade Commission, and other related sector-specific risk management agencies, support the development of guidance and risk profiles to help organizations utilize the privacy risk management framework developed pursuant to paragraph (1), to the extent practicable, to adopt privacy requirements and regulations established by the Federal Government, States, and international policymakers;

''(4) support activities to improve the efficacy and applicability of privacy-preserving computing, de-identification techniques and processes, and other technological means of mitigating individuals' privacy risks by enhancing predictability, manageability, disassociability, and confidentiality;

''(5) support and strategically engage in the development of voluntary, consensus-based technical standards for privacy-enhanced systems and networks, including international technical standards,

through open, transparent, and consensus-based processes; and

''(6) conduct such other activities as determined necessary by the Director to help public and private sector organizations mitigate the privacy risks associated with information systems and networks.''.

SEC. 602. NATIONAL PRIVACY AWARENESS AND EDUCATION INITIATIVE.

(a) NATIONAL PRIVACY AWARENESS AND EDUCATION INITIATIVE.—The Director of the National Institute of Standards and Technology, in consultation and collaboration with relevant Federal agencies, State, local, and Tribal governments, industry, educational institutions, civil society, and other nonprofit organizations, as appropriate, shall carry out privacy-related education and public awareness activities, including—

(1) the widespread dissemination of privacy-related technical standards and best practices identified by the Director;

(2) efforts to make privacy-related technical standards and best practices usable by individuals, small-to-medium-sized businesses, educational institutions, and State, local, and Tribal governments;

(3) activities to increase the awareness of privacy risks, individual privacy rights, and responsibilities; and

(4) supporting the development of technical standards and best practices to describe privacy-related tasks, knowledge, skills, abilities, competencies, and work roles to guide career development, education, and training activities in industry, academia, nonprofit organizations, and the Federal Government, including support for credentialing.

(b) CONSIDERATIONS.—In carrying out the authority described in subsection (a), the Director of the National Institute of Standards and Technology, in consultation with appropriate Federal agencies, shall leverage, to the extent practicable, the national cybersecurity awareness and education program under section 303 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7443).

(c) BIENNIAL BRIEFINGS.—Not later than one year after the date of the enactment of this Act and biennially thereafter, the Director of the National Institute of Standards and Technology shall brief the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives on the activities carried out pursuant to subsection (a).

(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $3,000,000 for each of fiscal years 2024 through 2028.

SEC. 603. NATIONAL SCIENCE FOUNDATION PRIVACY RESEARCH.

The Director of the National Science Foundation shall make awards on a competitive basis to institutions of higher education or non-profit organizations (or consortia of such institutions or organizations) to support multidisciplinary and transdisciplinary socio-technical research to design, prototype, and translate to practice privacy-preserving technologies and increase understanding of the human, social, behavioral, and economic dimensions of such potential technologies, including research on the following:

(1) Public understanding, expectations, and perspectives on privacy.

(2) Consumer privacy rights, including right to access, correction, deletion, data portability, individual autonomy, impermanence, and to be informed.

(3) Privacy governance and transparency, including notice and consent processes and the efficacy of privacy policies.

(4) Empowering consumers for data ownership and control.

(5) Privacy by design.

(6) Privacy-preserving automated decision-making systems and human review of automated decision-making systems.

(7) Ensuring privacy in consumer surveillance systems.

(8) User interfaces, including design elements that deliberately obscure, mislead, coerce, or deceive consumers.

(9) Privacy implications of emerging technologies.

(10) Incentives to implement privacy protections.

○