AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

116TH CONGRESS
2D SESSION

S. 3300

To establish a Federal data protection agency, and for other purposes.

IN THE SENATE OF THE UNITED STATES

FEBRUARY 13, 2020

Mrs. GILLIBRAND introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To establish a Federal data protection agency, 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) IN GENERAL.—This Act may be cited as the ''Data Protection Act of 2020''.

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

SEC. 2. FINDINGS AND PURPOSE.

(a) FINDINGS.—Congress finds the following:

(1) Privacy is an important fundamental individual right protected by the Constitution of the United States.

(2) The right of privacy is widely recognized in international legal instruments that the United States has endorsed, ratified, or promoted.

(3) The right to privacy protects the individual against intrusions into seclusion, protects individual autonomy, safeguards fair processing of data that pertains to the individual, advances the just processing of data, and contributes to respect for individual civil rights and fundamental freedoms.

(4) Privacy protections not only protect and benefit the individual, but they also advance other societal interests, including the protection of marginalized and vulnerable groups of individuals, the safeguarding of other foundational values of our democracy, such as freedom of information, freedom of speech, justice, and human ingenuity and dignity, as well as the integrity of democratic institutions, including fair and open elections.

(5) The privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal data.

(6) The increasing digitalization of information and its application in classifying individuals and groups of individuals has greatly magnified the harm to individual privacy that can occur from the collection, maintenance, use, or dissemination of personal data.

(7) The opportunities for an individual to secure employment, insurance, credit, and housing and the right to due process and other legal protections are endangered by the unrestricted collection, disclosure, processing, and misuse of personal data.

(8) Information systems lacking privacy protection amplify bias.

(9) In order to protect the privacy of individuals, it is necessary and proper for Congress to regulate the collection, maintenance, use, processing, storage, and dissemination of information.

(b) PURPOSE.—The purpose of this Act is to establish a data protection agency to—

(1) safeguard privacy, promote innovation, ensure compliance with the law, and promote best practices;

(2) provide guidance on matters related to electronic data storage, communication, and usage;

(3) provide the public with information and guidance on privacy protections and fair information practices and principles;

(4) oversee Federal agencies' implementation of section 552a of title 5, United States Code;

(5) promote implementation of fair information practices in the public and private sector; and

(6) represent the United States in international forums.

SEC. 3. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''Agency'' means the Data Protection Agency established under section 4.

(2) COVERED ENTITY.—The term ''covered entity'' means any person that collects, processes, or otherwise obtains personal data with the exception of an individual processing personal data in the course of personal or household activity.

(3) FEDERAL PRIVACY LAW.—

(A) IN GENERAL.—The term ''Federal privacy law'' means the provisions of this Act, the laws specified in subparagraph (B), and any rule or order prescribed by the Agency under

this Act or pursuant to the authorities transferred under this Act. Such term shall not include the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(B) SPECIFIED LAWS.—The laws specified in this subparagraph are the following laws (including any amendments made by such laws):

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

(ii) The CAN–SPAM Act of 2003 (15 U.S.C 7701 et seq.).

(iii) The Do-Not-Call Implementation Act (15 U.S.C. 6152 et seq.) and Public Law 108–82 (15 U.S.C. 6151).

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

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

(vi) Subtitle D of the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17921 et seq.).

(vii) The Identity Theft Assumption and Deterrence Act of 1998 (Pub. L. 105–318).

(viii) The Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. 6101 et seq.).

(ix) Section 227 of the Communications Act of 1934 (47 U.S.C. 227) (commonly known as the ''Telephone Consumer Protection Act of 1991'').

(4) HIGH-RISK DATA PRACTICE.—The term ''high-risk data practice'' means an action by a covered entity that involves—

(A) a systematic or extensive evaluation of personal data that is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or household or similarly significantly affect the individual or household;

(B) sensitive data uses;

(C) a systemic monitoring of publicly accessible data on a large scale;

(D) processing involving the use of new technologies, or combinations of technologies, that creates adverse consequences or potential adverse consequences to an individual or society;

(E) decisions about an individual's access to a product, service, opportunity, or benefit which is based to any extent on automated processing;

(F) any profiling of individuals on a large scale;

(G) any processing of biometric data for the purpose of uniquely identifying an individual;

(H) any processing of genetic data, other than data processed by a health care professional for the purpose of providing health care to the individual;

(I) combining, comparing, or matching personal data obtained from multiple sources;

(J) processing the personal data of an individual that has not been obtained directly from the individual;

(K) processing which involves tracking an individual's geolocation; or

(L) the use of personal data of children or other vulnerable individuals for marketing purposes, profiling, or automated processing.

(5) PERSONAL DATA.—The term ''personal data'' means any information that identifies, relates

to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or device, including—

(A) an identifier such as a real name, alias, signature, date of birth, gender identity, sexual orientation, marital status, physical characteristic or description, postal address, telephone number, unique personal identifier, military identification number, online identifier, Internet Protocol address, email address, account name, mother's maiden name, social security number, driver's license number, passport number, or other similar identifiers;

(B) information such as employment status, employment history, or other professional or employment-related information;

(C) bank account number, credit card number, debit card number, insurance policy number, or any other financial information;

(D) medical information, mental health information, or health insurance information;

(E) commercial information, including records of personal property, products or services purchased, obtained, or considered, or other

purchasing or consuming histories or tendencies;

(F) characteristics of protected classes under Federal law, including race, color, national origin, religion, sex, age, or disability;

(G) biometric information;

(H) internet or other electronic network activity information, including browsing history, search history, content, and information regarding an individual's interaction with an internet website, mobile application, or advertisement;

(I) historical or real-time geolocation data;

(J) audio, electronic, visual, thermal, olfactory, or similar information;

(K) education records;

(L) political information;

(M) password-protected digital photographs and digital videos not otherwise available to the public;

(N) information on criminal convictions or arrests;

(O) information (such as an Internet Protocol address or other similar identifier) that allows an individual or device to be singled out

for interaction, even without identification of such individual or device; and

(P) inferences drawn from any of the information identified in this subparagraph to create a profile about an individual reflecting the individual's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(6) PROCESS.—The term ''process'' means to perform an operation or set of operations on personal data, either manually or by automated means, including but not limited to collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, sorting, classifying, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.

(7) PROFILE.—The term ''profile'' means the use of an automated means to process data (including personal data and other data) to derive, infer, predict, or evaluate information about an individual or group, such as the processing of data to analyze or predict an individual's identity, attributes, interests, or behavior.

(8) SENSITIVE DATA USE.—The term ''sensitive data use'' means—

(A) the processing of data in a manner that reveals an individual's race, color, ethnicity, religion or creed, national origin or ancestry, sex, gender, gender identity, sexuality, sexual orientation, political beliefs, trade union membership, familial status, lawful source of income, financial status (such as the individual's income or assets), veteran status, criminal convictions or arrests, citizenship, past, present, or future physical or mental health or condition, psychological states, disability, geospatial data, or any other factor used as a proxy for identifying any of these characteristics; or

(B) the use of the biometric or genetic data of an individual.

(9) TRANSFER DATE.—The term ''transfer date'' means the date that is 1 year after the date of enactment of this Act.

SEC. 4. ESTABLISHMENT OF THE DATA PROTECTION AGENCY.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—There is established in the Executive branch an agency to be known as the

''Data Protection Agency'' which shall regulate the processing of personal data.

(2) STATUS.—The Agency shall be an independent establishment (as defined in section 104 of title 5, United States Code).

(b) DIRECTOR AND DEPUTY DIRECTOR.—

(1) IN GENERAL.—There is established a position of the Director of the United States Data Protection Agency (referred to in this Act as 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 from among members of the public at large who are well qualified for service on the Agency by virtue of their knowledge and expertise in—

(A) technology;

(B) protection of personal data;

(C) civil rights and liberties;

(D) law;

(E) social sciences; and

(F) business.

(4) 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 Federal Transit Administrator the following new item:

''Director of the United States Data Protection Agency.''.

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

(A) be appointed by the Director; and

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

(c) TERM.—

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

(2) 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.

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

(d) SERVICE RESTRICTION.—No Director or Deputy Director may engage in any other employment during the period of service of such person as Director or Deputy Director.

(e) OFFICES.—The principal office of the Agency shall be in the District of Columbia. The Director may establish regional offices of the Agency.

SEC. 5. EXECUTIVE AND ADMINISTRATIVE POWERS.

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

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

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

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

(4) to coordinate and oversee the operation of all administrative, enforcement, and research activities of the Agency;

(5) to adopt and use a seal;

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

(7) the appointment and supervision of personnel employed by the Agency;

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

(9) the use and expenditure of funds;

(10) implementing this Act and the Federal privacy laws through rules, orders, guidance, interpretations, statements of policy, examinations, 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 Agency by law.

(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.

SEC. 6. PURPOSE, OBJECTIVES, AND FUNCTIONS OF THE AGENCY.

(a) PURPOSE.—The Agency shall seek to protect individuals' privacy and limit the collection, disclosure, processing, and misuse of individuals' personal data by covered entities, and is authorized to exercise its authorities under this Act for such purposes.

(b) FUNCTIONS.—The primary functions of the agency are—

(1) providing leadership and coordination to the efforts of all Federal departments and agencies to enforce all Federal statutes, Executive orders, regulations and policies which involve privacy or data protection;

(2) maximizing effort, promoting efficiency, and eliminating conflict, competition, duplication, and inconsistency among the operations, functions, and jurisdictions of Federal departments and agencies responsible for privacy or data protection, data protection rights and standards, and fair information practices and principles;

(3) providing active leadership, guidance, education, and appropriate assistance to private sector businesses, and organizations, groups, institutions, and individuals regarding privacy, data protection rights and standards, and fair information practices and principles;

(4) requiring and overseeing ex-ante impact assessments and ex-post outcomes audits of high-risk data practices by covered entities to advance fair and just data practices;

(5) examining the social, ethical, economic, and civil rights impacts of high-risk data practices and propose remedies;

(6) ensuring that privacy practices and processing are fair, just, and comply with fair information practices;

(7) ensuring fair contract terms in the market, including the prohibition of ''pay-for-privacy provisions'' and ''take-it-or leave it'' terms of service;

(8) promoting privacy enhancing techniques, such as privacy by design and data minimization techniques;

(9) collecting, researching, and responding to consumer complaints;

(10) initiating a formal public rulemaking process at the Agency before any new high-risk data practice or other related profiling technique can be implemented;

(11) reviewing and approving new high-risk techniques or applications, giving special consideration to minors and sensitive data uses;

(12) regulating consumer scoring and other business practices that pertain 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;

(13) developing model privacy, data protection, and fair information practices, standards, guidelines, policies, and routine uses for use by the private sector;

(14) issuing rules, orders, and guidance implementing Federal privacy law;

(15) upon written request, providing appropriate assistance to the private sector in implementing privacy, data protection, and fair information practices, principles, standards, guidelines, policies, or routine uses of privacy and data protection, and fair information; and

(16) enforce other privacy statutes and rules as authorized by Congress.

SEC. 7. RULEMAKING AUTHORITY.

(a) IN GENERAL.—The Agency is authorized to exercise its authorities under this Act and Federal privacy law to administer, enforce, and otherwise implement the provisions of this Act and Federal privacy law.

(b) RULEMAKING, ORDERS, AND GUIDANCE.—

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

jectives of this Act and Federal privacy law, and to prevent evasions thereof.

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

(3) STANDARDS FOR RULEMAKING.—In prescribing a rule under the Federal privacy laws—

(A) the Agency shall consider—

(i) the potential benefits and costs to individuals or groups of individuals; and

(ii) the impact of proposed rules on individuals or groups of individuals;

(B) the Agency may provide that a rule shall only apply to a subcategory of covered entities, as defined by the Agency; and

(C) the Agency shall consult with civil society groups and members of the public.

(c) MONITORING.—In order to support its rulemaking and other functions, the Agency shall monitor for risks to individuals in the collection, disclosure, processing, and misuse of personal data.

SEC. 8. SPECIFIC AGENCY AUTHORITIES.

(a) SUPERVISION OF VERY LARGE COVERED ENTITIES.—

(1) IN GENERAL.—This subsection shall apply to any covered entity that satisfies one or more of the following thresholds:

(A) The entity has annual gross revenues that exceed $25,000,000.

(B) The entity annually buys, receives for the covered entity's commercial purposes, sells, or discloses for commercial purposes, alone or in combination, the personal information of 50,000 or more individuals, households, or devices.

(C) The entity derives 50 percent or more of its annual revenues from the sale of personal data.

(2) SUPERVISION.—The Agency may require reports and conduct examinations on a periodic basis of covered entities described in paragraph (1) for purposes of—

(A) assessing compliance with the requirements of Federal privacy laws;

(B) obtaining information about the activities subject to such laws and the associated compliance systems or procedures of such entities;

(C) detecting and assessing associated risks to individuals and groups of individuals; and

(D) requiring and overseeing ex-ante impact assessments and ex-post outcome audits of high-risk data practices to advance fair and just data practices.

(b) PROHIBITING UNFAIR OR DECEPTIVE ACTS AND PRACTICES.—

(1) IN GENERAL.—The Agency may take any action authorized under this Act to prevent a covered entity from committing or engaging in an unfair or deceptive act or practice (as defined by the Agency under this subsection) in connection with the collection, disclosure, processing, and misuse of personal data.

(2) RULEMAKING.—The Agency may prescribe rules applicable to a covered entity identifying as unlawful, unfair, or deceptive acts or practices in connection with the collection, disclosure, processing, and misuse of personal data. Rules under this section may include requirements for the purpose of preventing such acts or practices.

(3) UNFAIRNESS.—

(A) IN GENERAL.—The Agency shall have no authority under this section to declare an act or practice in connection with the collection, disclosure, processing, and misuse of personal data to be unlawful on the grounds that such act or practice is unfair, unless the Agency has a reasonable basis to conclude that—

(i) the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers; and

(ii) such substantial injury is not outweighed by countervailing benefits to consumers or to competition.

(B) CONSIDERATION OF PUBLIC POLICIES.—In determining whether an act or practice is unfair, the Agency may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

(c) RESPONSE TO CONSUMER COMPLAINTS AND INQUIRIES.—

(1) TIMELY REGULATOR RESPONSE TO CONSUMERS.—The Agency shall establish, in consulta-

tion with the appropriate Federal regulatory agencies, reasonable procedures to provide a timely response to consumers, in writing where appropriate, to complaints against, or inquiries concerning, a covered entity, including—

(A) steps that have been taken by the regulator in response to the complaint or inquiry of the consumer;

(B) any responses received by the regulator from the covered entity; and

(C) any follow-up actions or planned follow-up actions by the regulator in response to the complaint or inquiry of the consumer.

(2) TIMELY RESPONSE TO REGULATOR BY COVERED ENTITY.—A covered entity subject to supervision and primary enforcement by the Agency pursuant to this Act shall provide a timely response to the Agency, in writing where appropriate, concerning a consumer complaint or inquiry, including—

(A) steps that have been taken by the covered entity to respond to the complaint or inquiry of the consumer;

(B) responses received by the covered entity from the consumer; and

(C) follow-up actions or planned follow-up actions by the covered entity to respond to the complaint or inquiry of the consumer.

(3) ROUTING COMPLAINTS TO STATES.—To the extent practicable, State agencies may receive appropriate complaints from the systems established by the Agency under this subsection, if—

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

(B) 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

(C) 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.

SEC. 9. ENFORCEMENT POWERS.

(a) JOINT INVESTIGATIONS.—The Agency or, where appropriate, an Agency investigator, may engage in joint

investigations and requests for information, as authorized under this Act.

(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 paragraph 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 this subsection may be punished by the court as a contempt thereof.

(c) LITIGATION AUTHORITY.—

(1) IN GENERAL.—If any covered entity violates a Federal privacy law, the Agency may commence a civil action against such covered entity to impose a

civil penalty or to seek all appropriate legal and equitable relief including a permanent or temporary injunction as permitted by law.

(2) REPRESENTATION.—The Agency may act in its own name and through its own attorneys in enforcing any provision of this Act, rules thereunder, or any other law or regulation, or in any action, suit, or proceeding to which the Agency is a party.

(3) COMPROMISE OF ACTIONS.—The Agency may compromise or settle any action if such compromise is approved by the court.

(4) NOTICE TO THE ATTORNEY GENERAL.—

(A) IN GENERAL.—When commencing a civil action under Federal privacy law, or any rule thereunder, the Agency shall notify the Attorney General.

(B) NOTICE AND COORDINATION.—

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

(ii) COORDINATION.—In order to avoid conflicts and promote consistency re-

garding 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 by not later than 180 days after the transfer date. The agreement under this clause shall include provisions to ensure that parallel investigations and proceedings involving the Federal privacy laws are conducted in a manner that avoids conflicts and does not impede the ability of the Attorney General to prosecute violations of Federal criminal laws.

(iii) RULE OF CONSTRUCTION.—Nothing in this subparagraph shall be construed to limit the authority of the Agency under this Act, including the authority to interpret Federal privacy law.

(5) FORUM.—Any civil action brought under this Act may be brought in a United States district court or in any court of competent jurisdiction of a state in a district in which the defendant is located or resides or is doing business, and such court shall

have jurisdiction to enjoin such person and to require compliance with any Federal privacy law.

(6) TIME FOR BRINGING ACTION.—

(A) IN GENERAL.—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 an action relates.

(B) LIMITATIONS UNDER OTHER FEDERAL LAWS.—

(i) IN GENERAL.—An action arising under this Act does not include claims arising solely under the Federal privacy laws.

(ii) AGENCY AUTHORITY.—In any action arising solely under a Federal privacy law, the Agency may commence, defend, or intervene in the action in accordance with the requirements of that provision of law, as applicable.

(iii) TRANSFERRED AUTHORITY.—In any action arising solely under laws for which authorities were transferred under this Act, the Agency may commence, defend, or intervene in the action in accord-

ance with the requirements of that provision of law, as applicable.

(d) RELIEF AVAILABLE.—

(1) JURISDICTION.—The court (or the Agency, as the case may be) in an action or adjudication proceeding brought under Federal privacy law, shall have jurisdiction to grant any appropriate legal or equitable relief with respect to a violation of Federal privacy law, including a violation of a rule or order prescribed under a Federal privacy law.

(2) RELIEF.—Relief under this section may include, without limitation—

(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 covered entity; and

(H) civil money penalties, as set forth more fully in subsection (f).

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

(e) RECOVERY OF COSTS.—In any action brought by the Agency, a State attorney general, or any State regulator to enforce any Federal privacy law, the Agency, the State attorney general, or the State regulator may recover its costs in connection with prosecuting such action if the Agency, the State attorney general, or the State regulator is the prevailing party in the action.

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

(1) IN GENERAL.—Any person that violates, through any act or omission, any provision of Federal privacy law shall forfeit and pay a civil penalty pursuant to this subsection.

(2) PENALTY AMOUNTS.—

(A) FIRST TIER.—For any violation of a law, rule, or final order or condition imposed in writing by the Agency, a civil penalty may not exceed $5,000 for each day during which such violation or failure to pay continues.

(B) SECOND TIER.—Notwithstanding subparagraph (A), for any person that recklessly

engages in a violation of a Federal privacy law, a civil penalty may not exceed $25,000 for each day during which such violation continues.

(C) THIRD TIER.—Notwithstanding subparagraphs (A) and (B), for any person that knowingly violates a Federal privacy law, a civil penalty may not exceed $1,000,000 for each day during which such violation continues.

(3) MITIGATING FACTORS.—In determining the amount of any penalty assessed under paragraph (2), the Agency or the court 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 or failure to pay;

(C) the severity of the risks to or losses of the individual or group of individuals affected by the violation;

(D) the history of previous violations; and

(E) such other matters as justice may require.

(4) AUTHORITY TO MODIFY OR REMIT PENALTY.—The Agency may compromise, modify, or remit any penalty which may be assessed or had al-

ready been assessed under paragraph (2). The amount of such penalty, when finally determined, shall be exclusive of any sums owed by the covered entity 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 covered entity charged.

(5) NOTICE AND HEARING.—No civil penalty may be assessed under this subsection with respect to a violation of any Federal privacy law, unless—

(A) the Agency 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.

(g) REFERRALS 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.

(h) DATA PROTECTION RELIEF FUND.—

(1) ESTABLISHMENT OF RELIEF FUND.—There is established in the Treasury of the United States a separate fund to be known as the ''Data Protection Relief Fund'' (referred to in this subsection as the ''Relief Fund'').

(2) DEPOSITS.—

(A) DEPOSITS FROM THE AGENCY.—The Agency shall deposit into the Relief Fund the amount of any civil penalty obtained against any covered entity in any judicial or administrative action the Agency commences to enforce this Act, a regulation promulgated under this Act, or a Federal privacy law.

(B) DEPOSITS FROM THE ATTORNEY GENERAL.—The Attorney General of the United States shall deposit into the Relief Fund the amount of any civil penalty obtained against any covered entity in any judicial or administrative action the Attorney General commences on behalf of the Agency to enforce this Act, a regulation promulgated under this Act, or a Federal privacy law.

(3) USE OF FUND AMOUNTS.—Notwithstanding section 3302 of title 31, United States Code, amounts in the Relief Fund shall be available to the

Agency, without fiscal year limitation, to provide redress, payments or compensation, or other monetary relief to individuals affected by an act or practice for which civil penalties have been obtained under this Act. To the extent that individuals cannot be located or such redress, payments or compensation, or other monetary relief are otherwise not practicable, the Agency may use such funds for the purpose of consumer or business education relating to data protection or for the purpose of engaging in technological research that the Agency considers necessary to enforce this Act and Federal privacy laws.

(4) AMOUNTS NOT SUBJECT TO APPORTIONMENT.—Notwithstanding any other provision of law, amounts in the Relief Fund shall not be subject to apportionment for purposes of chapter 15 of title 31, United States Code, or under any other authority.

SEC. 10. PRESERVATION OF STATE LAW.

(a) RELATION TO STATE LAW.—

(1) RULE OF CONSTRUCTION.—This Act may not be construed as annulling, altering, or affecting, or exempting any person subject to the provisions of this title from complying with, the statutes, regulations, orders, or interpretations in effect in any State, except to the extent that any such provision

of law is inconsistent with the provisions of this title, and then only to the extent of the inconsistency.

(2) GREATER PROTECTION UNDER STATE LAW.—For purposes of this paragraph, a statute, regulation, order, or interpretation in effect in any State is not inconsistent with the provisions of this title if the protection that such statute, regulation, order, or interpretation affords to individuals is greater than the protection provided under this Act. A determination regarding whether a statute, regulation, order, or interpretation in effect in any State is inconsistent with the provisions of this title may be made by the Agency on its own motion or in response to a nonfrivolous petition initiated by any interested person.

(b) RELATION TO OTHER PROVISIONS OF FEDERAL PRIVACY LAWS THAT RELATE TO STATE LAW.—No provision of this Act shall be construed as modifying, limiting, or superseding the operation of any provision of a Federal privacy law that relates to the application of a law in effect in any State with respect to such Federal law.

(c) PRESERVATION OF ENFORCEMENT POWERS OF STATES.—The attorney general (or the equivalent thereof) of any State may bring a civil action in the name of such State in any district court of the United States in that

State or in State court that is located in that State and that has jurisdiction over the defendant, to enforce provisions of this title or regulations issued under this Act, and to secure remedies under provisions of this title or remedies otherwise provided under other law. A State regulator may bring a civil action or other appropriate proceeding to enforce the provisions of this title or regulations issued under this Act with respect to any entity that is State-chartered, incorporated, licensed, or otherwise authorized to do business under State law (except as provided in paragraph (2)), and to secure remedies under provisions of this title or remedies otherwise provided under other provisions of law with respect to such an entity.

(d) PRESERVATION OF STATE AUTHORITY.—

(1) STATE CLAIMS.—No provision of this section shall be construed as altering, limiting, or affecting the authority of a State attorney general or any other regulatory or enforcement agency or authority to bring an action or other regulatory proceeding arising solely under the law in effect in that State.

(2) STATE CONSUMER PROTECTION, PRIVACY, AND DATA REGULATORS.—No provision of this title shall be construed as altering, limiting, or affecting the authority of a State consumer protection, data

protection, or privacy agency (or any agency or office performing like functions) under State law to adopt rules, initiate enforcement proceedings, or take any other action with respect to a person regulated by such commission or authority.

SEC. 11. REPORTS AND INFORMATION.

(a) REPORTS REQUIRED.—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.

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

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

(2) 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;

(3) 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;

(4) 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 8 during the preceding 6-month period;

(5) 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

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

SEC. 12. TRANSFERS OF FUNCTIONS.

(a) FEDERAL TRADE COMMISSION.—The authority of the Federal Trade Commission under a Federal privacy law specified in section 3(3)(B) 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 transfer date. Nothing in this title shall be construed to

require a mandatory transfer of any employee of the Federal Trade Commission.

(b) AGENCY AUTHORITY.—

(1) IN GENERAL.—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 Federal Trade Commission on the day before the transfer date.

(2) FEDERAL TRADE COMMISSION ACT.—The Agency may enforce a rule prescribed under the Federal Trade Commission Act (45 U.S.C. 41 et seq.) by the Federal Trade Commission with respect to the collection, disclosure, processing, and misuse of personal data.

(c) AUTHORITY OF THE FEDERAL TRADE COMMISSION.—No provision of this title shall be construed as modifying, limiting, or otherwise affecting the authority of the Federal Trade Commission (including its authority with respect to very large entities described in section 8(a)(1)) under the Federal Trade Commission Act or any other law, other than the authority under a Federal privacy law to prescribe rules, issue official guidelines, or conduct a study or issue a report mandated under such law.

(d) AUTHORITY OF THE CONSUMER FINANCIAL PROTECTION BUREAU.—No provision of this title shall be construed as modifying, limiting, or otherwise affecting the authority of the Consumer Financial Protection Bureau under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Public Law 111–203) or any other law.

SEC. 13. AUTHORIZATION OF APPROPRIATIONS.

For fiscal year 2020 and each subsequent fiscal year, there are authorized to be appropriated to the Agency such sums as may be necessary to carry out this Act.

○