II

116TH CONGRESS
1ST SESSION

S. 583

To provide for digital accountability and transparency.

IN THE SENATE OF THE UNITED STATES

FEBRUARY 27, 2019

Ms. CORTEZ MASTO introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To provide for digital accountability and transparency.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Digital Accountability and Transparency to Advance Privacy Act'' or the ''DATA Privacy Act''.

SEC. 2. DEFINITIONS.

(a) IN GENERAL.—In this Act:

(1) COLLECT.—The term ''collect'' means taking any operation or set of operations to obtain covered data, including by automated means, including

purchasing, leasing, assembling, recording, gathering, acquiring, or procuring.

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

(3) COVERED DATA.—The term ''covered data''—

(A) means any information that is—

(i) collected, processed, stored, or disclosed by a covered entity;

(ii) collected over the internet or other digital network; and

(iii)(I) linked to an individual or device associated with an individual; or

(II) practicably linkable to an individual or device associated with an individual, including by combination with separate information, by the covered entity or any potential recipient of the data; and

(B) does not include data that is—

(i) collected, processed, stored, or disclosed solely for the purpose of employment of an individual; and

(ii) lawfully made available to the public from Federal, State, or local government records.

(4) COVERED ENTITY.—The term ''covered entity''—

(A) means any entity that collects, processes, stores, or discloses covered data; and

(B) does not include any entity that collects, processes, stores, or discloses covered data relating to fewer than 3,000 individuals and devices during any 12-month period.

(5) DISCLOSE.—The term ''disclose'' means taking any action with respect to covered data, including by automated means, to sell, share, provide, or otherwise transfer covered data to another entity, person, or the general public.

(6) PRIVACY RISK.—The term ''privacy risk'' means potential harm to an individual resulting from the collection, processing, storage, or disclosure of covered data, including—

(A) direct or indirect financial loss;

(B) stigmatization or reputational harm;

(C) anxiety, embarrassment, fear, and other severe emotional trauma;

(D) loss of economic opportunity; or

(E) physical harm.

(7) PROCESS.—The term ''process'' means any operation or set of operations that is performed on

covered data or on sets of covered data, including by automated means, including organizing, combining, adapting, altering, using, or transforming.

(8) PROTECTED CHARACTERISTIC.—The term ''protected characteristic'' means an individual's race, sex, gender, sexual orientation, nationality, religious belief, or political affiliation.

(9) PSEUDONYMOUS DATA.—The term ''pseudonymous data'' means covered data that may only be linked to the identity of an individual or the identity of a device associated with an individual if combined with separate information.

(10) REASONABLE INTEREST.—The term ''reasonable interest'' means—

(A) a compelling business, operational, administrative, legal, or educational justification for the collection, processing, storage, or disclosure of covered data exists;

(B) the use of covered data is within the context of the relationship between the covered entity and the individual linked to the covered data; and

(C) the interest does not subject the individual to an unreasonable privacy risk.

(11) SENSITIVE DATA.—The term ''sensitive data'' means any covered data relating to—

(A) the health, biologic, physiologic, biometric, sexual life, or genetic information of an individual; or

(B) the precise geolocation information of a device associated with an individual.

(12) STORE.—The term ''store'' means any operation or set of operations to continue possession of covered data, including by automated means.

(13) THIRD PARTY SERVICE PROVIDER.—The term ''third party service provider'' means any covered entity that collects, processes, stores, or discloses covered data at the direction of, and for the sole benefit of, another covered entity under a contract.

(b) MODIFIED DEFINITION BY RULEMAKING.—If the Commission determines that a term defined in paragraph (9) or (11) is not sufficient to protect an individual's data privacy, the Commission may promulgated regulations under section 553 of title 5, United States Code, to modify the definition as the Commission considers appropriate.

SEC. 3. REQUIRED PRIVACY NOTICE.

(a) PRIVACY NOTICE.—Each covered entity shall post in an accessible location a notice that is concise, in context, in easily understandable language, accurate, clear, timely, updated, uses visualizations where appropriate, conspicuous, and free of charge regarding the covered entity's privacy practices.

(b) CONTENTS OF NOTICE.—The notice required by subsection (a) shall include—

(1) a description of the covered data that the entity collects, processes, stores, and discloses, including the sources that provided the covered data if the covered entity did not collect the covered data;

(2) the purposes for and means by which the entity collects, processes, and stores the covered data;

(3) the persons and entities to whom, and purposes for which, the covered entity discloses the covered data; and

(4) a conspicuous, clear, and understandable means for individuals to access the methods necessary to exercise their rights under sections 4 and 5.

SEC. 4. REQUIRED DATA PRACTICES.

(a) REGULATIONS.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, that require covered entities to implement, practice, and maintain certain data procedures and processes that meet the following requirements:

(1) MINIMUM DATA PROCESSING REQUIREMENTS.—Except as provided in subsection (b), require covered entities to meet all of the following requirements regarding the means by and purposes for which covered data is collected, processed, stored, and disclosed:

(A) REASONABLE.—Except as provided in paragraph (3), covered data collection, processing, storage, and disclosure practices must meet a reasonable interest of the covered entity, including—

(i) business, educational, and administrative operations that are relevant and appropriate to the context of the relationship between the covered entity and the individual linked to the covered data;

(ii) relevant and appropriate product and service development and enhancement;

(iii) preventing and detecting abuse, fraud, and other criminal activity;

(iv) reasonable communications and marketing practices that follow best practices, rules, and ethical standards;

(v) engaging in scientific, medical, or statistical research that follows commonly accepted ethical standards; or

(vi) any other purpose for which the Commission considers to be reasonable.

(B) EQUITABLE.—Covered data collection, processing, storage, and disclosure practices may not be for purposes that result in discrimination against a protected characteristic, including—

(i) discriminatory targeted advertising practices;

(ii) price, service, or employment opportunity discrimination; or

(iii) any other practice the Commission considers likely to result in unfair discrimination against a protected characteristic.

(C) FORTHRIGHT.—Covered data collection, processing, storage, and disclosure practices may not be accomplished with means or for purposes that are deceptive, including—

(i) the use of inconspicuous recording or tracking devices and methods;

(ii) the disclosure of covered data that a reasonable individual believes to be the content of a private communication with another party or parties;

(iii) notices, interfaces, or other representations likely to mislead consumers; or

(iv) any other practice that the Commission considers likely to mislead individuals regarding the purposes for and means by which covered data is collected, processed, stored, or disclosed.

(2) REQUIREMENTS FOR OPT-OUT CONSENT.—Except as provided in subsection (b), require covered entities to provide individuals with conspicuous access to a method that is in easily understandable language, concise, accurate, clear, to opt out of any collection, processing, storage, or disclosure of covered data linked to the individual.

(3) REQUIREMENTS FOR AFFIRMATIVE CONSENT.—Except as provided in subsection (b), require covered entities to provide individuals with a notice that is concise, in easily understandable language, accurate, clear, timely, and conspicuous to express affirmative, opt-in consent—

(A) before the covered entity collects or discloses sensitive data linked to the individual; or

(B) before the covered entity collects, processes, stores, or discloses data for purposes which are outside the context of the relationship of the covered entity with the individual linked to the data, including—

(i) the use of covered data beyond what is necessary to provide, improve, or market a good or service that the individual requests;

(ii) the processing or disclosure of covered data differs in material ways from the purposes described in the privacy policy that was in effect when the data was collected; and

(iii) any other purpose that Commission considers outside of context.

(4) DATA MINIMIZATION REQUIREMENTS.—Except as provided in subsection (b), require covered entities to—

(A) take reasonable measures to limit the collection, processing, storage, and disclosure of covered data to the amount that is necessary to carry out the purposes for which the data is collected; and

(B) store covered data only as long as is reasonably necessary to carry out the purposes for which the data was collected.

(b) EXEMPTIONS.—Subsection (a) shall not apply if the limitations on the collection, processing, storage, or disclosure of covered data would—

(1) inhibit detection or prevention of a security risk or incident;

(2) risk the health, safety, or property of the covered entity or individual; or

(3) prevent compliance with an applicable law (including regulations) or legal process.

SEC. 5. INDIVIDUAL CONTROL OVER DATA USE.

(a) REGULATIONS.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to require covered entities to provide conspicuous, understandable, clear, and free of charge method to—

(1) upon the request of an individual, provide the individual with access to, or an accurate representation of, covered data linked to with the indi-

vidual or the individual's device stored by the covered entity;

(2) upon the request of an individual, provide the individual with a means to dispute and resolve the accuracy or completeness of the covered data linked to the individual or the individual's device stored by the entity;

(3) upon the request of an individual, delete any covered data that the covered entity stores linked to the individual or the individual's device; and

(4) when technically feasible, upon the request of an individual, allow the individual to transmit or transfer covered data linked to the individual or the individual's device that is maintained by the entity to the individual in a format that is standardized and interoperable.

(b) PSEUDONYMOUS DATA.—If the covered data that an individual has requested processed under subsection (a) is pseudonymous data, a covered entity may decline the request if processing the request is not technically feasible.

(c) TIMELINESS OF REQUESTS.—In fulfilling any requests made by the individual under subsection (a) the covered entity shall act in as timely a manner as is reasonably possible.

(d) ACCESS TO SAME SERVICE.—A covered entity shall not discriminate against an individual because of any action the individual took under their rights described in subsection (a), including—

(1) denying goods or services to the individual;

(2) charging, or advertising, different prices or rates for goods or services; or

(3) providing different quality of goods or services.

(e) CONSIDERATION.—The Commission shall allow a covered entity, by contract, to provide relevant obligations to the individual under subsection (a) on behalf of a third party service provider that collects, processes, stores, or discloses covered data only on behalf of the covered entity.

SEC. 6. INFORMATION SECURITY STANDARDS.

(a) REQUIRED DATA SECURITY PRACTICES.—

(1) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to require covered entities to establish and implement policies and procedures regarding information security practices for the treatment and protection of covered data taking into consideration—

(A) the level of identifiability of the covered data and the associated privacy risk;

(B) the sensitivity of the covered data collected, processed, and stored and the associated privacy risk;

(C) the currently available and widely accepted technological, administrative, and physical means to protect personal data under the control of the covered entity;

(D) the cost associated with implementing, maintaining, and regularly reviewing the safeguards; and

(E) the impact of these requirements on small and medium-sized businesses.

(2) LIMITATIONS.—In promulgating the regulations required under this section, the Commission shall consider a covered entity who is in compliance with existing information security laws that the Commission determines are sufficiently rigorous to be in compliance with this section with respect to particular types of covered data to the extent those types of covered data are covered by such law, including the following:

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

(B) The Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931).

(C) The Health Insurance Portability and Accountability Act of 1996 Security Rule (45 CFR 160.103 and part 164).

(D) Any other existing law requiring a covered entity to implement and maintain information security practices and procedures that the Commission determines to be sufficiently rigorous.

SEC. 7. PRIVACY PROTECTION OFFICERS.

(a) APPOINTMENT OF A PRIVACY PROTECTION OFFICER.—Each covered entity with annual revenue in excess of $25,000,000 the prior year shall designate at least 1 appropriately qualified employee as a privacy protection officer who shall—

(1) educate employees about compliance requirements;

(2) train employees involved in data processing;

(3) conduct regular, comprehensive audits to ensure compliance and make records of the audits available to enforcement authorities upon request;

(4) maintain updated, clear, and understandable records of all data security practices undertaken by the covered entity;

(5) serve as the point of contact between the covered entity and enforcement authorities; and

(6) advocate for policies and practices within the covered entity that promote individual privacy.

(b) PROTECTIONS.—The privacy protection officer shall not be dismissed or otherwise penalized by the covered entity for performing any of the tasks assigned to the person under this section.

SEC. 8. RESEARCH INTO PRIVACY ENHANCING TECHNOLOGY.

Section 4(a) of the Cyber Security Research and Development Act (15 U.S.C. 7403(a)) is amended—

(1) by striking the subsection heading and inserting the following:

"(a) NETWORK SECURITY AND INFORMATION PRIVACY RESEARCH GRANTS.—"; and

(2) in paragraph (1), by striking subparagraph (D) and inserting the following:

"(D) privacy and confidentiality, including—

"(i) cryptography;

"(ii) anonymization;

"(iii) pseudonymization;

"(iv) filtering tools;

"(v) anti-spying and anti-tracking tools; and

"(vi) any other technology that the Director determines will enhance individual privacy;".

SEC. 9. ENFORCEMENT.

(a) ENFORCEMENT BY THE COMMISSION.—

(1) IN GENERAL.—Except as otherwise provided, this Act and the regulations prescribed under this Act shall be enforced by the Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(2) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act or a regulation prescribed under this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(3) ACTIONS BY THE COMMISSION.—Subject to paragraph (4), the Commission shall prevent any person from violating this Act or a regulation prescribed under this Act in the same manner, by the

same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act, and any person who violates this Act or such regulation shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(4) COMMON CARRIERS.—Notwithstanding section 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), and 46) or any jurisdictional limitation of the Commission, the Commission shall also enforce this Act, in the same manner provided in paragraphs (1), (2), and (3) with respect to common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and Acts amendatory thereof and supplementary thereto.

(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) IN GENERAL.—

(A) CIVIL ACTIONS.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates this Act or a regulation prescribed under this Act, the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to—

(i) enjoin that practice;

(ii) enforce compliance with this Act or such regulation;

(iii) obtain damages, restitution, or other compensation on behalf of residents of the State;

(iv) impose a civil penalty in an amount that is not greater than the product of the number of individuals whose information was affected by a violation and $40,000; or

(v) obtain such other relief as the court may consider to be appropriate.

(B) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is after 1 year after the date of enactment of this Act, and each year thereafter, the amounts specified in subparagraph (A)(iv) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(C) NOTICE.—

(i) IN GENERAL.—Before filing an action under subparagraph (A), the attorney general of the State involved shall provide to the Commission—

(I) written notice of that action; and

(II) a copy of the complaint for that action.

(ii) EXEMPTION.—

(I) IN GENERAL.—Clause (i) shall not apply with respect to the filing of an action by an attorney general of a State under this paragraph if the attorney general determines that it is not feasible to provide the notice described in that clause before the filing of the action.

(II) NOTIFICATION.—In an action described in subclause (I), the attorney general of a State shall provide notice and a copy of the complaint to the Commission at the same time as the attorney general files the action.

(c) RIGHTS OF THE COMMISSION.—

(1) INTERVENTION BY THE COMMISSION.—The Commission may intervene in any civil action brought by the attorney general of a State under subsection (b) and upon intervening—

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

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

(2) POWERS.—Nothing in this subsection may be construed to prevent the attorney general of a State from exercising the powers conferred on the attorney general by the laws of the State to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

(3) ACTION BY THE COMMISSION.—If the Commission institutes a civil action for violation of this title or a regulation promulgated under this title, no attorney general of a State may bring a civil action under subsection (b) against any defendant named

in the complaint of the Commission for violation of this Act or a regulation promulgated under this Act that is alleged in the complaint.

(d) VENUE AND SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (b) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

(2) SERVICE OF PROCESS.—In an action brought under subsection (b), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

(e) ACTION OF OTHER STATE OFFICIALS.—

(1) IN GENERAL.—In addition to civil actions brought by attorneys general under subsection (b), any other officer of a State who is authorized by the State to do so may bring a civil action under subsection (b), subject to the same requirements and limitations that apply under this subsection to civil actions brought by attorneys general.

(2) SAVINGS PROVISION.—Nothing in this subsection may be construed to prohibit an authorized official of a State from initiating or continuing any proceeding in a court of the State for a violation of any civil or criminal law of the State.

(f) PRESERVATION OF AUTHORITY.—Nothing in this Act shall be construed to limit the authority of the Federal Trade Commission under any other provision of law.

SEC. 10. ADDITIONAL ENFORCEMENT RESOURCES.

(a) IN GENERAL.—Notwithstanding any other provision of law the Commission may, without regard to the civil service laws (including regulations), appoint not more than 300 additional personnel for the purposes of enforcing privacy and data security laws and regulations.

(b) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Commission such sums as may be necessary to carry out this section.

○