[~115H6864]

.....

(Original Signature of Member)

116TH CONGRESS
1ST SESSION

H. R. _____

To require the Federal Trade Commission to promulgate regulations related to sensitive personal information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Ms. DELBENE introduced the following bill; which was referred to the Committee on _____

A BILL

To require the Federal Trade Commission to promulgate regulations related to sensitive personal information, 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.

This Act may be cited as the ''Information Transparency & Personal Data Control Act''.

SEC. 2. SENSE OF CONGRESS.

It is the Sense of Congress that—

(1) the United States must develop a balanced, high-standard digital framework that establishes global standards;

(2) a key element of this framework is a strong national standard that combats anti-consumer practices;

(3) it is critical that the Federal Government provide guidance on the collection and storage of sensitive data;

(4) it is important to provide our country with fair and thoughtful digital consumer rights; and

(5) it is important to ensure that our enforcement authorities have the resources needed to protect consumers from bad actors in the privacy and security space.

SEC. 3. REQUIREMENTS FOR SENSITIVE PERSONAL INFORMATION.

(a) REGULATIONS.—Not later than 1 year after the date of the enactment of this Act, the Federal Trade Commission shall promulgate regulations under section 553 of title 5, United States Code, to require, except as provided in subsection (b), any controller that provides services to the public involving the collection, storage, processing, sale, sharing with third parties, or other use of sensitive personal information from United States persons or per-

sons located in the United States when the data is collected, to meet the following requirements:

(1) AFFIRMATIVE, EXPRESS, AND OPT-IN CONSENT.—Provide users with notice through a privacy and data use policy of a specific request to use their sensitive personal information and require that users provide affirmative, express, and opt-in consent to any functionality that involves the collection, storage, processing, sale, sharing, or other use of sensitive personal information, including sharing sensitive personal information with third parties.

(2) PRIVACY AND DATA USE POLICY.—Provide users with an up-to-date, transparent privacy, security, and data use policy that meets general requirements, including that such policy, presented to users in the context where it applies—

(A) is concise and intelligible;

(B) is clear and prominent in appearance;

(C) uses clear and plain language;

(D) uses visualizations where appropriate to make complex information understandable by the ordinary user; and

(E) is provided free of charge.

(3) ADDITIONAL REQUIREMENTS FOR PRIVACY AND DATA USE POLICY.—The privacy, security, and

data use policy required under paragraph (2) shall include the following:

(A) Identity and contact information of the entity collecting the sensitive personal information.

(B) The purpose or use for collecting, storing, processing, selling, sharing, or otherwise using the sensitive personal information.

(C) Third parties with whom the sensitive personal information will be shared and for what purposes.

(D) The storage period for how long the sensitive personal information will be retained by the controller and any third party, as applicable.

(E) How consent to collecting, storing, processing, selling, sharing, or otherwise using the sensitive personal information, including sharing with third parties, may be withdrawn.

(F) How a user can view or obtain the sensitive personal information that they have provided to a controller and whether it can be exported to other web-based platforms.

(G) What kind of sensitive personal information is collected and shared.

(H) Whether the sensitive personal information will be used to create profiles about users and whether they will be integrated across platforms.

(I) How sensitive personal information is protected from unauthorized access or acquisition.

(4) OPT-OUT CONSENT.—For any collection, storage, processing, selling, sharing, or other use of non-sensitive personal information, including sharing with third parties, controllers shall provide users with the ability to opt out at any time.

(5) PRIVACY AUDITS.—

(A) IN GENERAL.—Except as provided in subparagraphs (C) and (D), annually, each controller collecting, storing, processing, selling, sharing, or otherwise using sensitive personal information shall—

(i) obtain a privacy audit from a qualified, objective, independent third-party; and

(ii) shall make public whether or not the privacy audit found the controller compliant.

(B) AUDIT REQUIREMENTS.—Each such audit shall—

(i) set forth the privacy, security, and data use controls that the controller has implemented and maintained during the reporting period;

(ii) describe whether such controls are appropriate to the size and complexity of the controller, the nature and scope of the activities of the controller, and the nature of the sensitive personal information or behavioral data collected by the controller;

(iii) certify whether the privacy and security controls operate with sufficient effectiveness to provide reasonable assurance to protect the privacy and security of sensitive personal information or behavioral data, including with respect to data shared with third parties, and that the controls have so operated throughout the reporting period;

(iv) be prepared and completed within 60 days after the end of the reporting period to which the audit applies; and

(v) be provided to the Federal Trade Commission or to the attorney general of a State, or other authorized State officer, within 10 days of notification by the Commission or the attorney general of a State, or other authorized State officer where such person has presented to the controller allegations that a violation of this Act or any regulation issued under this Act has been committed by the controller.

(C) SMALL BUSINESS AUDIT EXEMPTION.—The audit requirements described in this paragraph shall not apply to controllers who collect, store, process, sell, share, or otherwise use sensitive personal information relating to 5,000 or fewer individuals.

(D) NON-SENSITIVE PERSONAL INFORMATION EXEMPTION.—The audit requirements set forth above shall not apply to controllers who do not collect, store, process, sell, share, or otherwise use sensitive personal information.

(b) EXEMPTIONS.—

(1) NECESSARY OPERATIONS AND SECURITY PURPOSES.—Subsection (a) shall not apply to the processing, collecting, storing, sharing, selling of

sensitive personal information for the following purposes:

(A) Preventing or detecting fraud, identity theft, or criminal activity.

(B) The use of such information to identify errors that impair functionality or otherwise enhancing or maintaining the availability of the services or information systems of the controller for authorized access and use.

(C) Protecting the vital interests of the consumer or another natural person.

(D) Responding in good faith to valid legal process or providing information as otherwise required or authorized by law.

(E) Monitoring or enforcing agreements between the controller and an individual, including but not limited to, terms of service, terms of use, user agreements, or agreements concerning monitoring criminal activity.

(F) Protecting the property, services, or information systems of the controller against unauthorized access or use.

(G) Advancing a substantial public interest, including archival purposes, scientific or historical research, and public health, if such

processing does not create a significant risk of harm to consumers.

(2) REASONABLE EXPECTATION OF USERS.—The regulations promulgated pursuant to subsection (a) with respect to the requirement to provide opt-in consent shall not apply to the processing, storage, and collection of sensitive personal information or behavioral data in which such processing does not deviate from purposes consistent with a controller's relationship with users as understood by the reasonable user.

SEC. 4. APPLICATION AND ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) COMMON CARRIERS.—Notwithstanding the limitations in the Federal Trade Commission Act (15 U.S.C. 41 et seq.) on Commission authority with respect to common carriers, this Act applies, according to its terms, to common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof and supplementary thereto.

(b) ENFORCEMENT.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a rule under section 18(a)(1)(B) of the Fed-

eral Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION.—Except as provided in subsection (a), the Federal Trade Commission shall enforce this Act and the regulations promulgated 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. Any person who violates this Act or a regulation promulgated under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

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

SEC. 5. RIGHT OF ACTION.

(a) RIGHT OF ACTION.—Except as provided in subsection (e), the attorney general of a State, or other authorized State officer, alleging a violation of this Act or any regulation issued under this Act that affects or may affect such State or its residents may bring an action on

behalf of the residents of the State in any United States district court for the district in which the defendant is found, resides, or transacts business, or wherever venue is proper under section 1391 of title 28, to obtain appropriate injunctive relief.

(b) NOTICE TO COMMISSION REQUIRED.—A State shall provide prior written notice to the Federal Trade Commission of any civil action under subsection (a) together with a copy of its complaint, except that if it is not feasible for the State to provide such prior notice, the State shall provide such notice immediately upon instituting such action.

(c) INTERVENTION BY THE COMMISSION.—The Commission may intervene in such civil action and upon intervening—

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

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

(d) CONSTRUCTION.—Nothing in this section shall be construed—

(1) to prevent the attorney general of a State, or other authorized State officer, from exercising the powers conferred on the attorney general, or other

authorized State officer, by the laws of such State; or

(2) to prohibit the attorney general of a State, or other authorized State officer, from proceeding in State or Federal court on the basis of an alleged violation of any civil or criminal statute of that State.

(e) LIMITATION.—

(1) NO SEPARATE ACTION.—An action may not be brought under subsection (a) if the same alleged violation is the subject of a pending action by the Commission or the United States.

(2) EXCLUSIVE PERIOD TO ACT BY COMMISSION.—An action—

(A) may not be brought under subsection (a) until the expiration of the 60-day period that begins on the date on which a violation is discovered by the Commission or the date on which the Commission is notified of the violation; and

(B) may only be brought under subsection (a) if the Commission does not bring an action related to the violation during such period.

SEC. 6. PRIVACY AND DATA SECURITY EMPLOYEES AND FUNDING FOR THE COMMISSION.

(a) EMPLOYMENT AUTHORITY.—The Commission shall hire 50 new full-time employees to focus on privacy and data security, 15 of which shall have technology expertise.

(b) ADDITIONAL FUNDING FOR PRIVACY AND DATA SECURITY.—There is authorized to be appropriated to the Commission $35,000,000 for issues related to privacy and data security.

SEC. 7. DEFINITIONS.

In this Act:

(1) CALL DETAIL RECORD.—The term ''call detail record''—

(A) means session-identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call;

(B) does not include—

(i) the contents (as defined in section 2510(8) of title 18, United States Code) of any communication;

(ii) the name, address, or financial information of a subscriber or customer;

(iii) cell site location or global positioning system information; or

(iv) business customers.

(2) CLEAR AND PROMINENT.—The term ''clear and prominent'' means in any communication medium, the required disclosure is—

(A) of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend the communication;

(B) provided in a manner such that an ordinary consumer is able to read and comprehend the communication;

(C) is presented in an understandable language and syntax;

(D) includes nothing contrary to, inconsistent with, or that mitigates any statement contained within the disclosure or within any document linked to or referenced therein; and

(E) includes an option that is compliant with applicable obligations of the controller under title III of the Americans with Disabilities Act of 1990 (42 U.S.C. 12181 et seq.).

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

(4) CONTROLLER.—The term ''controller'' means a person that, on its own or jointly with other entities, determines the purposes and means of processing sensitive personal information.

(5) PROCESSOR.—The term ''processor'' means a person that processes data on behalf of the controller.

(6) SENSITIVE PERSONAL INFORMATION.—

(A) The term ''sensitive personal information'' means information relating to an identified or identifiable individual, including the following:

(i) Financial account information.

(ii) Health information.

(iii) Genetic data.

(iv) Information pertaining to children under 13 years of age.

(v) Social Security numbers.

(vi) Unique government-issued identifiers

(vii) Authentication credentials, such as a username and password.

(viii) Precise geolocation information.

(ix) Content of a wire communication, oral communication, or electronic communication with respect to any entity that is not the intended recipient of the communication.

(x) Call detail records.

(xi) Web browsing history, application usage history, and the functional equivalent of either.

(xii) Biometric information.

(xiii) Sexual orientation.

(xiv) Religious beliefs.

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

(i) de-identified information (or the process of transforming personal data so that it is not directly relatable to an identified or identifiable consumer);

(ii) information related to employment; or

(iii) publicly available information.

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

(8) THIRD PARTY.—The term ''third party'' means an individual or entity that uses or receives sensitive personal information or behavioral data obtained by or on behalf of a controller, other than—

(A) a service provider of a controller to whom the controller discloses the consumer's sensitive personal information for an operational purpose pursuant to an agreement that prohibits the service provider receiving the sensitive personal information from using or disclosing the sensitive personal information for the benefit of the provider; and

(B) any entity that uses sensitive personal information only as reasonably necessary—

(i) to comply with applicable law, regulation, or legal process;

(ii) to enforce the terms of use of a controller; or

(iii) to detect, prevent, or mitigate fraud or security vulnerabilities.

SEC. 8. RULE OF CONSTRUCTION.

Nothing in this Act may be construed to preclude the acquisition by the Federal Government of—

(1) the contents of a wire or electronic communication pursuant to other lawful authorities, includ-

ing the authorities under chapter 119 of title 18, United States Code (commonly known as the ''Wiretap Act''), the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), or any other provision of Federal law not specifically amended by this Act; or

(2) records or other information relating to a subscriber or customer of any electronic communication service or remote computing service (not including the content of such communications) pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), chapter 119 of title 18, United States Code (commonly known as the ''Wiretap Act''), or any other provision of Federal law not specifically amended by this Act.

SEC. 9. NATIONAL STANDARD.

(a) PREEMPTION.—For a controller that is subject to this Act, or any regulation promulgated pursuant to this Act, the provisions of this Act, or any such regulation, shall preempt any civil provision of the law of any State or political subdivision of a State to the degree the law is focused on the reduction of privacy risk through the regulation of the collection of sensitive personal information and the collection, storage, processing, sale, sharing with third parties, or other use of such information.

(b) CONSUMER PROTECTION LAWS.—Except as provided in subsection (a), this section may not be construed to limit the enforcement, or the bringing of a claim pursuant to any State consumer protection law by an attorney general of a State, other than the extent to which any such law regulates the collection of sensitive personal information and the collection, storage, processing, sale, sharing with third parties, or other use of such information.

(c) PROTECTION OF CERTAIN STATE LAW.—Nothing in this Act may be construed to preempt the applicability of any of the following:

(1) State constitutional, trespass, contract, data breach notification, or tort law, other than to the degree such law is substantially intended to govern the collection of sensitive personal information and the collection, storage, processing, sale, sharing with third parties, or other use of such information.

(2) Any other State law to the extent that the law relates to acts of fraud, wiretapping, or the protection of social security numbers.

(3) Any State law to the extent the law provides additional provisions to specifically regulate the covered entities as defined for purposes of the regulations promulgated pursuant to section 264(c) of

the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–191), section 444 of the General Education Provisions Act (commonly known as the Family Educational Rights and Privacy Act of 1974) (20 U.S.C. 1232g), the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), or the Gramm-Leach-Bliley Act (15 U.S.C. 6701 et seq.).

(4) Any private contract based on a State law that requires a party to provide additional or greater privacy for sensitive personal information or data security protections to an individual than this Act, or any regulation promulgated pursuant to this Act.

SEC. 10. EFFECTIVE DATE.

This Act shall take effect 180 days after the date of the enactment of this Act.