115TH CONGRESS  
2D SESSION  

H. R. _____

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

1 Be it enacted by the Senate and House of Representa-
2 tives of the United States of America in Congress assembled,

3 SECTION 1. SHORT TITLE.

4 This Act may be cited as the “Information Trans-
5 parency & Personal Data Control Act”.

(Original Signature of Member)
SEC. 2. REQUIREMENTS FOR SENSITIVE PERSONAL INFORMATION OR BEHAVIORAL DATA.

(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 operator 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 persons 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 data 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 personal data 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 personal information, including how the sensitive personal information is shared with third parties.

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

(D) The storage period for how long the personal information will be retained by the operator 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 the sensitive personal information that they have provided to an operator and whether it can be exported to other web-based platforms.

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

(H) Whether the sensitive personal information will be used to create profiles about users.

(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, Operators shall provide users with the ability to opt out at any time.

(5) PRIVACY AUDITS.—

(A) IN GENERAL.—Annually, Operators collecting, storing, processing, selling, sharing, or otherwise using sensitive personal informa-
tion shall obtain a privacy audit from an objective, independent third-party professional with substantial experience in the field of privacy and data protection, who uses procedures and standards generally accepted in such field.

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

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

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

(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 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 Operator allegations that a violation of this Act or any regulation issued under this Act has been committed by the Operator.

(C) SMALL BUSINESS EXEMPTION.—Notwithstanding other authorities of the FTC, the audit requirements set forth above shall not apply to Operators with 500 or fewer employees.

(D) NON-SENSITIVE PERSONAL INFORMATION EXEMPTION.—The audit requirements set forth above shall not apply to Operators 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.

(B) Protecting the security of people, devices, networks, or facilities.

(C) Protecting the health, safety, rights, or property of the covered entity or another 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 covered entity and an individual, including but not limited to, terms of service, terms of use, user agreements, or agreements concerning monitoring criminal activity.

(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 of sensitive personal information or behavioral data in which such processing does not deviate from purposes con-
consistent with an operator’s relationship with users as understood by the reasonable user.

SEC. 3. APPLICATION AND ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) GENERAL APPLICATION.—This Act applies, according to its terms, to those persons, partnerships, and corporations over which the Federal Trade Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)). Notwithstanding the limitations in the Federal Trade Commission Act on Commission authority with respect to common carriers, this Act also applies, according to its terms, 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.—

(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 regulation under section 18(a)(1)(B) of the Federal 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 Commis-
sion 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. 4. 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; or

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

(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 operator.
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) **OPERATOR.**—The term “operator” means any entity who operates a website located on the internet or an online service and who collects or maintains personal information from or about individuals, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any entity that buys and sells consumer data without direct consumer interaction, and any entity offering products or services for sale through that website or online service, involving commerce among the States or with 1 or more foreign nations.

(5) **SENSITIVE PERSONAL INFORMATION.**—The term “sensitive personal information” means information relating to an identified or identifiable individual, including the following:

(A) Financial information.

(B) Health information.

(C) Relationships.

(D) Information pertaining to children under 13 years of age.
(E) Social Security numbers.

(F) Driver’s license or other government-issued identification number.

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

(H) Precise geolocation information.

(I) Content of communications.

(J) Call detail records.

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

(L) Biometric information.

(M) Sexual orientation.

(N) Political preferences.

(O) Religious beliefs.

(P) Any other personal or behavioral information that the Commission determines to be sensitive.

(6) 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.

(7) 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 an operator, other than—

(A) a service provider of an operator to whom the operator discloses the consumer’s sensitive personal information for an operational purpose pursuant to an agreement that prohibits the person receiving the personal information from using or disclosing the personal information for any purpose other than the purposes contemplated by the agreement; and

(B) any entity that uses such data only as reasonably necessary—

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

(ii) to enforce an operator’s terms of use; or

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

SEC. 5. RULE OF CONSTRUCTION.

Nothing in this Act shall 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, including the authorities under chapter 119 of title 18, United States Code (commonly known as the “Wire-
tap 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 ‘‘Wire-tap Act’’), or any other provision of Federal law not specifically amended by this Act.

SEC. 6. 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) to-
gether 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 insti-
tuting such action.

(c) INTERVENTION BY THE COMMISSION.—The Com-
mission may intervene in such civil action and upon inter-
vening—

(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 vio-
lation of any civil or criminal statute of that State.
(e) LIMITATION.—No separate suit shall be brought under this section if, at the time the suit is brought, the same alleged violation is the subject of a pending action by the Federal Trade Commission or the United States under this chapter.

SEC. 7. EFFECTIVE DATE.

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