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.

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 “Online Transparency & Personal Data Control Act”.

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

(a) Regulations.—Not later than 90 days 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 or behavioral data 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, or other use of sensitive personal information or behavioral data, including sharing personal data with third parties.

(2) Privacy and data use policy.—Provide users with an up-to-date, transparent privacy and data use policy that meets general requirements, in-
cluding 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 and data use
policy required under paragraph (2) shall include the
following:

(A) Identity and contact information of the
entity collecting the sensitive personal informa-
tion or behavioral data.

(B) The purpose or use for collecting, stor-
ing, processing, or otherwise using the data, in-
cluding how the data is shared with third par-
ties.

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

(D) The storage period for how long the
data will be retained by the operator and any
third party, as applicable.
(E) How consent to collecting, storing, processing, or otherwise using the data, including sharing with third parties, may be withdrawn.

(F) How a user can view their personal history and whether it can be exported to other web-based platforms.

(G) What kind of sensitive personal information or behavioral data, if any, is required to be provided for discrete functions or applications to work and what happens if that information is not provided.

(H) Whether the data will be profiled or automatically processed.

(4) PRIVACY AUDITS.—

(A) IN GENERAL.—Not less frequently than every 2 years, obtain a privacy audit for the previous 2 years from an objective, independent third-party professional (with a minimum of 3 years of experience in the field of privacy and data protection), who uses procedures and standards generally accepted in such field and submit the audit to the Commission.

(B) AUDIT REQUIREMENTS.—Each such audit shall—
(i) set forth the specific privacy and
data use controls that the operator has im-
plemented and maintained during the re-
porting 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 sensi-
tivity of the sensitive personal information
or behavioral data collected by the oper-
ator;

(iii) certify whether the privacy con-
trols operate with sufficient effectiveness to
provide reasonable assurance to protect the
privacy of sensitive personal information or
behavioral data and that the controls have
so operated throughout the reporting pe-
riod;

(iv) be prepared and completed within
60 days after the end of the reporting pe-
riod to which the audit applies, and sub-
mitted to the Federal Trade Commission
upon the completion of the 60-day period;
(v) be subject to disclosure under section 552 of title 5, United States Code (commonly referred to as FOIA), except for privileged business information and any other exception described under subsection (b) of such section.

(C) REDACTED VERSION FOR DISCLOSURE.—Publish a redacted version (removing any information that would not be subject to disclosure under section 552 of title 5, Untied States Code) of any privacy audit submitted to the Commission.

(b) EXEMPTIONS.—

(1) TECHNICALLY NECESSARY OPERATIONS AND SECURITY PURPOSES.—The regulations promulgated pursuant to subsection (a) shall not apply to the processing of sensitive personal information or behavioral data that is performed in the course of technically necessary operations to provide the service a user has consented to or for security purposes.

(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 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 and the regulations promulgated under this Act apply, according to their 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)).

(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.—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 Com-
mission Act (15 U.S.C. 41 et seq.) were incorpor-
ated into and made a part of this Act. Any per-
son who violates this Act or a regulation promul-
gated under this Act shall be subject to the penalties
and entitled to the privileges and immunities pro-

SEC. 4. DEFINITIONS.

In this Act:

(1) CALL DETAIL RECORD.—The term “call de-
tail record”—

(A) means session-identifying information
(including an originating or terminating tele-
phone number, an International Mobile Sub-
scriber 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 in-
formation of a subscriber or customer; or

(iii) cell site location or global posi-
tioning system information.
(2) CLEAR AND PROMINENT.—The term “clear and prominent” means—

(A) in a textual communication (such as a printed publication or words displayed on the screen of a computer or mobile device), the required disclosure is—

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

(ii) in print that contrasts highly with the background on which the communication appears;

(B) in a communication disseminated orally or through audible means (such as radio or streaming audio), the required disclosure is delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend the communication;

(C) in a communication disseminated through video, the required disclosure is—

(i) in writing in a form consistent with subparagraph (A);

(ii) appears on the screen for a duration sufficient for an ordinary consumer to
read and comprehend the communication;
and

(iii) in the same language as the pre-
dominant language that is used in the
communication; and

(D) in each instance, the required disclo-
sure—

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

(ii) includes nothing contrary to, in-
consistent with, or that mitigates any
statement contained within the disclosure
or within any document linked to or ref-
ereeced therein; and

(iii) includes an alternative 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 indi-
viduals, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including 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 OR BEHAVIORAL DATA.—The term “sensitive personal information or behavioral data” means information relating to an identified or identifiable individual, including the following:

(A) A first and last name.

(B) A home or other physical address including street name and name of a city or town.

(C) IP address or other network identifier.

(D) Financial information.

(E) An e-mail address or functional equivalent.

(F) A telephone number.

(G) Health information.

(H) Relationships.

(I) Information pertaining to children under 18 years of age.

(J) Social Security numbers.
(K) Driver’s license or other government-issued identification number.

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

(M) Geolocation information.

(N) Content of communications.

(O) Any information about who a communication is sent to.

(P) Call detail records.

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

(R) Device identifiers.

(S) Biometric information.

(T) Sexual orientation.

(U) Political preferences.

(V) Religious beliefs.

(W) 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 that—

(i) uses such data for and at the direction of an operator (and no other individual or entity) and for no other purpose; and

(ii) does not disclose such data, or any individually identifiable information derived from such data, except for, and at the direction of, an operator, for the purpose of providing services requested by a user and for no other purpose; or

(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 “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. 6. EFFECTIVE DATE.

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