To establish duties for online service providers with respect to end user data that such providers collect and use.

IN THE SENATE OF THE UNITED STATES

Mr. SCHATZ (for himself, Ms. HASSAN, Mr. BENNET, Ms. DUCKWORTH, Ms. KLOBUCHAR, Mrs. MURRAY, Mr. BOOKER, Ms. CORTEZ MASTO, Mr. HEINRICH, Mr. MARKEY, Mr. BROWN, Ms. BALDWIN, Mr. JONES, Mr. MANCHIN, and Mr. DURBIN) introduced the following bill; which was read twice and referred to the Committee on 

A BILL

To establish duties for online service providers with respect to end user data that such providers collect and use.

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 “Data Care Act of 2018”.

SEC. 2. DEFINITIONS.

In this Act—

(1) the term “Commission” means the Federal Trade Commission;
(2) the term “end user” means an individual who engages with an online service provider or logs into or uses services provided by the online service provider over the internet or any other digital network;

(3) the term “individual identifying data” means any data that is—

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

(B) linked, or reasonably linkable, to—

(i) a specific end user; or

(ii) a computing device that is associated with or routinely used by an end user;

(4) the term “online service provider” means an entity that—

(A) is engaged in interstate commerce over the internet or any other digital network; and

(B) in the course of business, collects individual identifying data about end users, including in a manner that is incidental to the business conducted; and

(5) the term “sensitive data” means any data that includes—

(A) a social security number;
(B) personal information (as defined in section 1302 of the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. 6501)) collected from a child (as defined in such section 1302);

(C) a driver’s license number, passport number, military identification number, or any other similar number issued on a government document used to verify identity;

(D) a financial account number, credit or debit card number, or any required security code, access code, or password that is necessary to permit access to a financial account of an individual;

(E) unique biometric data such as a fingerprint, voice print, a retina or iris image, or any other unique physical representation;

(F) information sufficient to access an account of an individual, such as user name and password or email address and password;

(G) the first and last name of an individual, or first initial and last name, or other unique identifier in combination with—

(i) the month, day, and year of birth of the individual;
(ii) the maiden name of the mother of the individual; or

(iii) the past or present precise geolocation of the individual;

(H) information that relates to—

(i) the past, present, or future physical or mental health or condition of an individual; or

(ii) the provision of health care to an individual; and

(I) the nonpublic communications or other nonpublic user-created content of an individual.

SEC. 3. PROVIDER DUTIES.

(a) In General.—An online service provider shall fulfill the duties of care, loyalty, and confidentiality under paragraphs (1), (2), and (3), respectively, of subsection (b).

(b) Duties.—

(1) Duty of Care.—An online service provider shall—

(A) reasonably secure individual identifying data from unauthorized access; and

(B) subject to subsection (c), promptly in-
scribed in subparagraph (A) of this paragraph with respect to sensitive data of that end user.

(2) DUTY OF LOYALTY.—An online service provider may not use individual identifying data, or data derived from individual identifying data, in any way that—

(A) will benefit the online service provider to the detriment of an end user; and

(B)(i) will result in reasonably foreseeable and material physical or financial harm to an end user; or

(ii) would be unexpected and highly offensive to a reasonable end user.

(3) DUTY OF CONFIDENTIALITY.—An online service provider—

(A) may not disclose or sell individual identifying data to, or share individual identifying data with, any other person except as consistent with the duties of care and loyalty under paragraphs (1) and (2), respectively;

(B) may not disclose or sell individual identifying data to, or share individual identifying data with, any other person unless that person enters into a contract with the online service provider that imposes on the person the
same duties of care, loyalty, and confidentiality
toward the applicable end user as are imposed
on the online service provider under this sub-
section; and

(C) shall take reasonable steps to ensure
that the practices of any person to whom the
online service provider discloses or sells, or with
whom the online service provider shares, indi-
vidual identifying data fulfill the duties of care,
loyalty, and confidentiality assumed by the per-
son under the contract described in subpara-
graph (B), including by auditing, on a regular
basis, the data security and data information
practices of any such person.

(c) Expansion of Duty to Inform Regarding
Breaches.—The Commission may promulgate regula-
tions under section 553 of title 5, United States Code,
to apply the breach notification requirement under sub-
section (b)(1)(B) with respect to specific categories of in-
dividual identifying data other than sensitive data, as the
Commission determines necessary.

(d) Exceptions.—

(1) Regulations.—The Commission may pro-
mulgate regulations under section 553 of title 5,
United States Code, to exempt categories of online
service providers from the requirement under subsection (a).

(2) CONSIDERATIONS.—In promulgating regulations under paragraph (1), the Commission shall consider, among other factors—

(A) the privacy risks posed by the use of individual identifying data by an online service provider based on—

(i) the size of the provider;

(ii) the complexity of the offerings of the provider;

(iii) the nature and scope of the activities of the provider; and

(iv) the sensitivity of the consumer information handled by the provider; and

(B) the costs and benefits of applying the requirement under subsection (a) to online service providers with particular combinations of characteristics considered under subparagraph (A) of this paragraph.

SEC. 4. ENFORCEMENT.

(a) ENFORCEMENT BY COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 3 by an online service provider shall be treated as a violation of a rule de-
fining an unfair or deceptive act or practice pre-
scribed under section 18(a)(1)(B) of the Federal

(2) POWERS OF COMMISSION.—

(A) IN GENERAL.—Except as provided in
subparagraph (C), the Commission shall enforce
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.

(B) PRIVILEGES AND IMMUNITIES.—Ex-
cept as provided in subparagraph (C), any per-
son who violates section 3 shall be subject to
the penalties and entitled to the privileges and
immunities provided in the Federal Trade Com-
mission Act (15 U.S.C. 41 et seq.).

(C) NONPROFIT ORGANIZATIONS AND COM-
MON CARRIERS.—Notwithstanding section 4 or
5(a)(2) of the Federal Trade Commission Act
(15 U.S.C. 44, 45(a)(2)) or any jurisdictional
limitation of the Commission, the Commission
shall also enforce this Act, in the same manner
provided in subparagraphs (A) and (B) of this paragraph, with respect to—

(i) organizations not organized to carry on business for their own profit or that of their members; and

(ii) common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.).

(3) Rulemaking Authority.—The Commission shall promulgate regulations under this Act in accordance with section 553 of title 5, United States Code.

(b) Enforcement by States.—

(1) Authorization.—Subject to paragraph (3), in any case in which the attorney general of a State has reason to believe that an interest of the residents of the State has been or is threatened or adversely affected by the engagement of an online service provider in a practice that violates section 3, the attorney general of the State may, as parens patriae, bring a civil action against the online service provider on behalf of the residents of the State in an appropriate district court of the United States to obtain appropriate relief, including civil penalties in the amount determined under paragraph (2).
(2) Civil Penalties.—An online service provider that is found, in an action brought under paragraph (1), to have knowingly or repeatedly violated section 3 shall, in addition to any other penalty otherwise applicable to a violation of section 3, be liable for a civil penalty equal to the amount calculated by multiplying—

(A) the greater of—

   (i) the number of days during which the online service provider was not in compliance with that section; or
   (ii) the number of end users who were harmed as a result of the violation, by

   (B) an amount not to exceed the maximum civil penalty for which a person, partnership, or corporation may be liable under section 5(m)(1)(A) of the Federal Trade Commission Act (15 U.S.C. 45(m)(1)(A)) (including any adjustments for inflation).

(3) Rights of Federal Trade Commission.—

   (A) Notice to Federal Trade Commission.—

       (i) In general.—Except as provided in clause (iii), the attorney general of a
State shall notify the Commission in writing that the attorney general intends to bring a civil action under paragraph (1) before initiating the civil action.

(ii) CONTENTS.—The notification required under clause (i) with respect to a civil action shall include a copy of the complaint to be filed to initiate the civil action.

(iii) EXCEPTION.—If it is not feasible for the attorney general of a State to provide the notification required under clause (i) before initiating a civil action under paragraph (1), the attorney general shall notify the Commission immediately upon instituting the civil action.

(B) INTERVENTION BY FEDERAL TRADE COMMISSION.—The Commission may—

(i) intervene in any civil action brought by the attorney general of a State under paragraph (1); and

(ii) upon intervening—

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

(II) file petitions for appeal of a decision in the civil action.
(4) **Investigatory 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—

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary or other evidence.

(5) **Preemptive action by Federal Trade Commission.**—If the Commission institutes a civil action or an administrative action with respect to a violation of section 3, the attorney general of a State may not, during the pendency of the action, bring a civil action under paragraph (1) against any defendant named in the complaint of the Commission based on the same set of facts giving rise to the alleged violation with respect to which the Commission instituted the action.

(6) **Venue; service of process.**—

(A) **Venue.**—Any action brought under paragraph (1) may be brought in—

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

(ii) another court of competent jurisdiction.

(B) SERVICE OF PROCESS.—In an action brought under paragraph (1), process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

(7) ACTIONS BY OTHER STATE OFFICIALS.—

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

(B) 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.
SEC. 5. NONENFORCEABILITY OF CERTAIN PROVISIONS

WAIVING RIGHTS AND REMEDIES.

The rights and remedies provided under this Act may not be waived or limited by contract or otherwise.

SEC. 6. RELATION TO OTHER PRIVACY AND SECURITY LAWS.

Nothing in this Act may be construed to—

(1) modify, limit, or supersede the operation of any privacy or security provision in any other Federal or State statute or regulation; or

(2) limit the authority of the Commission under any other provision of law.

SEC. 7. EFFECTIVE DATE.

(a) IN GENERAL.—This Act shall take effect on the date of enactment of this Act.

(b) APPLICABILITY.—Section 3 shall apply with respect to an online service provider on and after the date that is 180 days after the date of enactment of this Act.