To protect the privacy of consumers’ personal health information, proximity
data, device data, and geolocation data during the coronavirus public
health crisis.

IN THE SENATE OF THE UNITED STATES

Mr. WICKER (for himself, Mr. THUNE, Mr. MORAN, Mrs. BLACKBURN, and
Mrs. FISCHER) introduced the following bill; which was read twice and
referred to the Committee on

A BILL

To protect the privacy of consumers’ personal health information, proximity
data, device data, and geolocation data during the coronavirus public health crisis.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the “COVID–19 Consumer
Data Protection Act of 2020”.

SEC. 2. DEFINITIONS.

In this Act:

(1) AGGREGATED DATA.—The term “aggre-
gated data” means information that—
(A) relates to a group or category of individuals; and

(B) does not identify, and is not linked or reasonably linkable to, any individual.

(2) **Affirmative express consent.**—

(A) **In general.**—The term “affirmative express consent” means an affirmative act by an individual that—

(i) clearly communicates the individual’s authorization of an act or practice; and

(ii) is taken after the individual has been presented with a clear and conspicuous description of such act or practice.

(B) **No inference from inaction.**—For purposes of subparagraph (A), the affirmative express consent of an individual cannot be inferred from inaction.

(3) **Business contact information.**—The term “business contact information” means information related to an individual’s business position name or title, business telephone number, business address, business email address, and other similar business information, provided that such information
is collected, processed, or transferred solely for purposes related to such individual’s professional activities.

(4) Collection.—The term “collection” means buying, renting, gathering, accessing, or otherwise acquiring any covered data of an individual by any means.


(6) Covered data.—

(A) In general.—The term “covered data” means precise geolocation data, proximity data, a persistent identifier, and personal health information.

(B) Exclusions.—Such term does not include the following:

(i) Aggregated data.

(ii) Business contact information.

(iii) De-identified data.

(iv) Employee screening data.

(v) Publicly available information.

(7) Covered entity.—The term “covered entity” means, with respect to a set of covered data, any entity or person that—

(A) is—
4

(i) subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.); or

(ii) a common carrier or nonprofit organization described in section 4(a)(4);

(B) collects, processes, or transfers such covered data, or determines the means and purposes for the collection, processing, or transfer of covered data; and

(C) is not a service provider with respect to such data.

(8) COVID–19 PUBLIC HEALTH EMERGENCY.—

The term “COVID–19 public health emergency” means the period—

(A) beginning on the date of enactment of this Act; and

(B) ending on the last day of the public health emergency declared by the Secretary of Health and Human Services pursuant to section 319 of the Public Health Service Act (42 U.S.C. 247d) on January 31, 2020, entitled “Determination that a Public Health Emergency Exists Nationwide as the Result of the 2019 Novel Coronavirus” (including any renewal of such declaration pursuant to such section 319).
(9) **De-identified Data.**—The term “de-identified data” means information held by a covered entity that—

(A) does not identify and is not reasonably linkable to an individual;

(B) does not contain any personal identifiers or other information that could be readily used to re-identify the individual to whom the information pertains;

(C) is subject to a public commitment by the covered entity—

(i) to refrain from attempting to use such information to identify any individual; and

(ii) to adopt technical and organizational measures to ensure that such information is not linked to any individual; and

(D) is not disclosed by the covered entity to any other party unless the disclosure is subject to a contractually or other legally binding requirement that—

(i) the recipient of the information shall not use the information to identify any individual; and
(ii) all onward disclosures of the information shall be subject to the requirement described in clause (i).

(10) EMPLOYEE SCREENING DATA.—The term “employee screening data” means, with respect to a covered entity, covered data of an individual who is an employee, owner, director, officer, staff member, trainee, vendor, visitor, intern, volunteer, or contractor of the covered entity, provided that such data is only collected, processed, or transferred by the covered entity for the purpose of determining, for purposes related to the COVID–19 public health emergency, whether the individual is permitted to enter a physical site of operation of the covered entity.

(11) DELETE.—The term “delete” means to remove or destroy information such that it is not maintained in human or machine readable form and cannot be retrieved or utilized in the normal course of business.

(12) INDIVIDUAL.—

(A) IN GENERAL.—The term “individual” means a natural person residing in the United States.
(B) EXCLUSION.—Such term does not include, with respect to a covered entity, an individual acting as a full-time or part-time, paid or unpaid employee, owner, director, officer, staff member, trainee, vendor, visitor, intern, volunteer, or contractor of a covered entity permitted to enter a physical site of operation of the covered entity.

(13) PERSISTENT IDENTIFIER.—The term “persistent identifier” means a technologically derived identifier that identifies an individual, or is linked or reasonably linkable to an individual over time and across services and platforms, which may include a customer number held in a cookie, a static Internet Protocol (IP) address, a processor or device serial number, or another unique device identifier.

(14) PERSONAL HEALTH INFORMATION.—

(A) IN GENERAL.—The term “personal health information” means information relating to an individual that—

(i) is—

(I) genetic information of the individual; or

(II) information relating to the diagnosis or treatment of past,
present, or future physical, mental health, or disability of the individual; and 

(ii) identifies, or is reasonably linkable to, the individual.

(B) EXCLUSIONS.—Such term does not include the following:

(i) Information from education records that are subject to the requirements of section 444 of the General Education Provisions Act (20 U.S.C. 1232g, commonly referred to as the “Family Educational Rights and Privacy Act of 1974”) or from records described in subsection (a)(4)(B)(iv) of such section.

(ii) Information subject to regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note).

(15) PRECISE GEOLOCATION DATA.—The term “precise geolocation data” means technologically derived information capable of determining with reasonable specificity the past or present actual phys-
(16) **Process.**—The term “process” means any operation or set of operations performed on covered data, including analyzing, organizing, structuring, retaining, using, or otherwise handling such data.

(17) **Proximity Data.**—The term “proximity data” means technologically derived information that identifies the past or present proximity of one individual to another.

(18) **Publicly Available Information.**—The term “publicly available information” means any information that—

(A) has been lawfully made available to the general public from Federal, State, or local government records; or

(B) is widely available to the general public, including information from—

(i) a telephone book or online directory;

(ii) video, internet, or audio content;

or

(iii) the news media or a website that is available to the general public on an un-
restricted basis (for purposes of this sub-
clause a website is not restricted solely be-
cause there is a fee or log-in requirement
associated with accessing the website).

(19) Service provider.—The term “service
provider” means, with respect to a set of covered
data, an entity that processes or transfers such cov-
ered data for the purpose of performing one or more
services or functions on behalf of, and at the direc-
tion of, a covered entity to which it is not related.

(20) Transfer.—The term “transfer” means
to disclose, release, share, disseminate, or otherwise
make available covered data by any means.

SEC. 3. PRIVACY OF COVERED DATA.

(a) In General.—During the COVID–19 public
health emergency, it shall be unlawful for a covered entity
to collect, process, or transfer the covered data of an indi-
vidual for a purpose described in subsection (b) unless—

(1) the covered entity provides the individual
with prior notice of the purpose for such collection,
processing, or transfer;

(2) the individual has given affirmative express
consent to such collection, processing, or transfer;
and
(3) the covered entity publicly commits not to collect, process, or transfer such covered data for a purpose other than the purpose described in subsection (b) to which the individual consented unless—

(A) such collection, processing, or transfer is necessary to comply with the provisions of this Act or other applicable laws;

(B) such collection, processing, or transfer is necessary to carry out operational or administrative tasks in support of a purpose described in subsection (b) to which the individual has consented; or

(C) the individual gives affirmative express consent to such collection, processing, or transfer.

(b) COVERED PURPOSES.—The purposes described in this subsection are the following:

(1) Collecting, processing, or transferring the covered data of an individual to track the spread, signs, or symptoms of COVID–19.

(2) Collecting, processing, or transferring the covered data of an individual to measure compliance with social distancing guidelines or other requirements related to COVID–19 that are imposed on in-
dividends under a Federal, State, or local govern-
ment order.

(3) Collecting, processing, or transferring the
covered data of an individual to conduct contact
tracing for COVID–19 cases.

(c) TRANSPARENCY.—

(1) PRIVACY POLICY.—A covered entity that
collects, processes, or transfers covered data for a
purpose described in subsection (b) shall, not later
than 14 days after the enactment of this Act, pub-
lish a privacy policy that—

(A) is disclosed in a clear and conspicuous
manner to an individual prior to or at the point
of the collection of covered data for such a pur-
pose from the individual;

(B) is made available in a clear and con-
spicuous manner to the public;

(C) includes whether, subject to the affirm-
ative express consent requirement of subsection
(a), the covered entity transfers covered data
for such a purpose and the categories of recipi-
ents to whom the covered entity transfers cov-
ered data for such purpose;

(D) includes a general description of the
covered entity’s data retention practices for cov-
erased data used for a purpose described in subsection (b) and the purposes for such retention; and

(E) includes a general description of the covered entity’s data security practices.

(2) REPORTING.—During the COVID–19 public health emergency, a covered entity that collects, processes, or transfers covered data for a purpose described in subsection (b) shall issue a public report not later than 30 days after the enactment of this Act and not less frequently than once every 60 days thereafter—

(A) stating in aggregate terms the number of individuals whose covered data the entity has collected, processed, or transferred for such a purpose; and

(B) describing the categories of covered data collected, processed, or transferred by the entity, the specific purposes for which each such category of covered data is collected, processed, or transferred, and, in the case of transferred covered data, to whom such data was transferred.

(d) RIGHT TO OPT-OUT.—During the COVID–19 public health emergency, each covered entity that collects,
processes, or transfers covered data for a purpose described in subsection (b) shall do the following:

(1) The covered entity shall provide an effective mechanism for an individual who has consented pursuant to subsection (a) to the collection, processing, or transfer of the individual’s covered data for such a purpose to revoke such consent.

(2) A covered entity that receives a revocation of consent from an individual described in paragraph (1) shall, as soon as practicable but in no case later than 14 days after receiving such revocation, stop collecting, processing, or transferring the covered data of such individual for a purpose described in subsection (b), or shall de-identify all such data.

(e) DATA DELETION.—A covered entity shall delete or de-identify all covered data collected, processed, or transferred for a purpose described in subsection (b) when it is no longer being used for such purpose and is no longer necessary to comply with a Federal, State, or local legal obligation, or the establishment, exercise, or defense of a legal claim.

(f) DATA ACCURACY.—A covered entity shall take reasonable measures to ensure the accuracy of covered data collected, processed, or transferred for a purpose described in subsection (b) and shall provide an effective
mechanism for an individual to report inaccuracies in covered data.

(g) Data Minimization.—

(1) In General.—During the COVID–19 public health emergency, a covered entity that collects, processes, or transfers covered data for a purpose described in subsection (b) shall not collect, process, or transfer covered data beyond what is reasonably necessary, proportionate, and limited to carry out such purpose.

(2) Guidelines.—Not later than 30 days after the date of enactment of this Act, the Commission shall issue guidelines recommending best practices for covered entities to minimize the collection, processing, and transfer of covered data in accordance with this subsection.

(h) Protection of Covered Data.—During the COVID–19 public health emergency, a covered entity that collects, processes, or transfers covered data for a purpose described in subsection (b) shall establish, implement, and maintain reasonable administrative, technical, and physical data security policies and practices to protect against risks to the confidentiality, security, and integrity of such data.
(i) EXCEPTION.—Notwithstanding subsection (a), a covered entity may collect, process, or transfer the covered data of an individual or group of individuals for a purpose described in subsection (b) during the COVID–19 public health emergency without obtaining the affirmative express consent of the individual if such collection, processing, or transfer is necessary to allow the covered entity to comply with a Federal, State, or local legal obligation.

SEC. 4. ENFORCEMENT.

(a) ENFORCEMENT BY FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of 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 paragraph (4), 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. Any person who violates such section shall
be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act. Except as provided in subsection (c), enforcement by the Commission shall be the exclusive means of enforcing compliance with this Act.

(3) Cooperation with other agencies.—Whenever the Commission obtains information that any covered entity may have processed or transferred covered data in violation of Federal anti-discrimination laws, the Commission shall transmit the information to the appropriate Federal or State agency with authority to initiate proceedings related to such violation.

(4) Common carriers and nonprofit organizations.—Notwithstanding section 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46) or any jurisdictional limitation of the Commission, the Commission shall also enforce this Act in the same manner provided in paragraphs (1) and (2) of this subsection with respect to—

(A) common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof and supplementary thereto; and
(B) organizations not organized to carry
on business for their own profit or that of their
members.

(b) Effect on Other Laws.—

(1) In general.—Nothing in this Act shall be construed in any way to limit the authority of the Commission under any other provision of law.

(2) Nonapplication of FCC Laws and Regulations to Covered Entities.—Notwithstanding any other provision of law, neither any provision of the Communications Act of 1934 (47 U.S.C. 151 et. seq.) and all Acts amendatory thereof and supplementary thereto nor any regulation promulgated by the Federal Communications Commission under such Acts shall apply to any covered entity with respect to the collection, processing, or transferring of covered data for a purpose described in section 3(b), except to the extent that such provision or regulation pertains solely to “911” lines or any other emergency line of a hospital, medical provider or service office, health care facility, poison control center, fire protection agency, or law enforcement agency.

(3) State Preemption.—No State or political subdivision of a State may adopt, maintain, enforce,
or continue in effect any law, regulation, rule, requirement, or standard to the extent that such law, regulation, rule, requirement, or standard is related to the collection, processing, or transfer of covered data for a purpose described in section 3(b).

(c) Enforcement by State Attorneys General.—

(1) In general.—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 adversely affected by the engagement of any covered entity in an act or practice that violates this Act, the attorney general of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to—

(A) enjoin that act or practice;

(B) enforce compliance with this Act or the regulation;

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

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

(2) Rights of the Commission.—
(A) IN GENERAL.—Except where not feasible, the attorney general of a State shall notify the Commission in writing prior to initiating a civil action under paragraph (1). Such notice shall include a copy of the complaint to be filed to initiate such action. Upon receiving such notice, the Commission may intervene in such action and, upon intervening—

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

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

(B) NOTIFICATION TIMELINE.—Where it is not feasible for the attorney general of a State to provide the notification required by subparagraph (A) before initiating a civil action under paragraph (1), the attorney general shall notify the Commission immediately after initiating the civil action.

(3) ACTIONS BY COMMISSION.—In any case in which a civil action is instituted by the Commission for violation of this Act, no attorney general of a State may, during the pendency of such action, institute a civil action against any defendant named in the complaint in the action instituted by the Com-
mission for a violation of this Act that is alleged in such complaint.

(4) INVESTIGATORY POWERS.—Nothing in this Act shall be construed to prevent the attorney general of a State or another authorized official of a State from exercising the powers conferred on the attorney general or the State official 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.

(5) CONSOLIDATION OF ACTIONS BROUGHT BY TWO OR MORE STATE ATTORNEYS GENERAL OR AUTHORIZED STATE GOVERNMENTAL AUTHORITIES.—Whenever a civil action under paragraph (1) is pending and another civil action or actions are commenced pursuant to such paragraph in a different Federal district court or courts that involve 1 or more common questions of fact, such action or actions shall be transferred for the purposes of consolidated pretrial proceedings and trial to the United States District Court for the District of Columbia; provided however, that no such action shall be transferred if pretrial proceedings in that action have been concluded before a subsequent action is filed by
a State attorney general or authorized State govern-
mental authority.