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

1 Be it enacted by the Senate and House of Representati- 
2 ves of the United States of America in Congress assembled, 
3 SECTION 1. SHORT TITLE. 
4 This Act may be cited as the “COVID–19 Consumer 
5 Data Protection Act of 2020”.
6 SEC. 2. DEFINITIONS. 
7 In this Act: 
8 (1) AGGREGATED DATA.—The term “aggregated data” means information that—

RD0 FL FGT
(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) COLLECTION.—The term “collection” means buying, renting, gathering, accessing, or otherwise acquiring any covered data of an individual by any means.

(4) COMMISSION.—The term “Commission” means the Federal Trade Commission.
(5) COVERED DATA.—The term “covered data” means precise geolocation data, proximity data, and personal health information.

(6) COVERED ENTITY.—The term “covered entity” means any entity or person that—

(A) is—

(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)(3); and

(B) collects, processes, or transfers covered data.

(7) 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).

(8) **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).

(9) 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.

(10) INDIVIDUAL.—The term “individual” means a natural person residing in the United States.

(11) 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 in-
clude the following:

(i) Information from education
records that are subject to the require-
ments of section 444 of the General Edu-
cation Provisions Act (20 U.S.C. 1232g,
commonly referred to as the “Family Edu-
cational 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 Acc-
countability Act of 1996 (42 U.S.C.
1320d–2 note).

(iii) Aggregated data.

(iv) De-identified data.

(v) Publicly available information.

(12) PRECISE GEOLOCATION DATA.—

(A) IN GENERAL.—The term “precise
golocation data” means technologically derived
information capable of determining with reasonable specificity the past or present actual physical location of an individual at a specific point in time.

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

(i) Aggregated data.

(ii) De-identified data.

(iii) Publicly available information.

(13) 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.

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

(15) 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 unrestricted basis (for purposes of this subclause a website is not restricted solely because there is a fee or log-in requirement associated with accessing the website).

(16) 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 individual 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, and transfer; and

(2) the individual has given 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 individuals under a Federal, State, or local government 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, publish 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 purpose from the individual;
(B) is made available in a clear and conspicuous manner to the public;

(C) includes whether, subject to the affirmative express consent requirement of subsection (a), the covered entity transfers covered data for such a purpose and the categories of recipients to whom the covered entity transfers covered data for such purpose;

(D) includes a general description of the covered entity’s data retention practices for covered 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, not less frequently than once every 30 days, issue a public report—

(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.

(f) **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.

(g) **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.
(h) 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 legal obligation.

SEC. 4. ENFORCEMENT.

(a) Enforcement by Federal Trade Commission.—

(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 Commission shall enforce this Act and any regulation 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 such section shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission 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 Executive 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 and any regulation promulgated under 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, 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, re-
quirement, or standard related to the collection,
processing, or transfer of covered data for a purpose
described in section 3(b).

(c) ENFORCEMENT BY STATE ATTORNEYS 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 en-
gagement of any covered entity that is not subject to the
Commission’s enforcement authority under subsection (a)
in an act or practice that violates this Act or a regulation
promulgated under 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—

(1) enjoin that act or practice;

(2) enforce compliance with this Act or the reg-
ulation;

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

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