116TH CONGRESS
2D SESSION

S. _____

To establish privacy requirements for operators of infectious disease exposure notification services.

IN THE SENATE OF THE UNITED STATES

Ms. CANTWELL (for herself and Mr. CASSIDY) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To establish privacy requirements for operators of infectious disease exposure notification services.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Exposure Notification Privacy Act''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.
Sec. 3. Public trust in automated exposure notification services.
Sec. 4. Voluntary participation and transparency.
Sec. 5. Data restrictions.
Sec. 6. Data deletion.

Sec. 7. Data security.
Sec. 8. Freedom of movement and nondiscrimination.
Sec. 9. Oversight.
Sec. 10. Enforcement.

SEC. 2. DEFINITIONS.

In this Act:

(1) AFFIRMATIVE EXPRESS CONSENT.—

(A) IN GENERAL.—The term ''affirmative express consent'' means an affirmative act by an individual that clearly communicates the individual's authorization for an act or practice, in response to a specific request that—

(i) is provided to the individual in a clear and conspicuous disclosure that is separate from other options or acceptance of general terms; and

(ii) includes a description of each act or practice for which the individual's consent is sought and—

(I) is written concisely and in easy-to-understand language; and

(II) includes a prominent heading that would enable a reasonable individual to identify and understand the act or practice.

(B) EXPRESS CONSENT REQUIRED.—Affirmative express consent shall not be inferred

from the inaction of an individual or the individual's continued use of a service or product.

(C) VOLUNTARY.—Affirmative express consent shall be freely given and nonconditioned.

(2) AGGREGATE DATA.—The term ''aggregate data'' means information that relates to a group or category of individuals that is not linked or reasonably linkable to any individual or device that is linked or reasonably linkable to an individual, provided that a platform operator or operator of an automated exposure notification service—

(A) takes reasonable measures to safeguard the data from reidentification;

(B) publicly commits in a conspicuous manner not to attempt to reidentify or associate the data with any individual or device linked or reasonably linkable to an individual;

(C) processes the data for public health purposes only; and

(D) contractually requires the same commitment for all transfers of the data.

(3) AUTHORIZED DIAGNOSIS.—The term ''authorized diagnosis'' means an actual, potential, or presumptive positive diagnosis of an infectious dis-

ease confirmed by a public health authority or a licensed health care provider.

(4) AUTOMATED EXPOSURE NOTIFICATION SERVICE.—

(A) IN GENERAL.—The term ''automated exposure notification service'' means a website, online service, online application, mobile application, or mobile operating system that is offered in commerce in the United States and that is designed, in part or in full, specifically to be used for, or marketed for, the purpose of digitally notifying, in an automated manner, an individual who may have become exposed to an infectious disease (or the device of such individual, or a person or entity that reviews such disclosures).

(B) LIMITATIONS.—Such term does not include—

(i) any technology that a public health authority uses as a means to facilitate traditional in-person, email, or telephonic contact tracing activities, or any similar technology that is used to assist individuals to evaluate if they are experiencing symptoms related to an infectious disease to the ex-

tent the technology is not used as an automated exposure notification service; or

(ii) any platform operator or service provider that provides technology to facilitate an automated exposure notification service to the extent the technology acts only to facilitate such services and is not itself used as an automated exposure notification service.

(5) COLLECT; COLLECTION.—The terms ''collect'' and ''collection'' mean buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means, including by passively or actively observing the behavior of an individual.

(6) COVERED DATA.—The term ''covered data'' means any information that is—

(A) linked or reasonably linkable to any individual or device linked or reasonably linkable to an individual;

(B) not aggregate data; and

(C) collected, processed, or transferred in connection with an automated exposure notification service.

(7) DECEPTIVE ACT OR PRACTICE.—The term ''deceptive act or practice'' means a deceptive act or practice in violation of section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)).

(8) DELETE.—The term ''delete'' means destroying, permanently erasing, or otherwise modifying covered data to make such covered data permanently unreadable or indecipherable and unrecoverable.

(9) EXECUTIVE AGENCY.—The term ''Executive agency'' has the meaning given such term in section 105 of title 5, United States Code.

(10) INDIAN TRIBE.—The term ''Indian tribe''—

(A) has the meaning given such term in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304); and

(B) includes a Native Hawaiian organization as defined in section 6207 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7517).

(11) OPERATOR OF AN AUTOMATED EXPOSURE NOTIFICATION SERVICE.—The term ''operator of an automated exposure notification service'' means any

person or entity that operates an automated exposure notification service, other than a public health authority, and that is—

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

(B) described in section 10(a)(4).

(12) PLATFORM OPERATOR.—The term ''platform operator'' means any person or entity other than a service provider who provides an operating system that includes features supportive of an automated exposure notification service and facilitates the use or distribution of such automated exposure notification service to the extent the technology is not used by the platform operator as an automated exposure notification service.

(13) PROCESS.—The term ''process'' means any operation or set of operations performed on covered data, including collection, analysis, organization, structuring, retaining, using, securing, or otherwise handling covered data.

(14) PUBLIC HEALTH AUTHORITY.—The term ''public health authority'' means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe that is responsible for public health mat-

ters as part of its official mandate, or a person or entity acting under a grant of authority from or contract with such public agency.

(15) SERVICE PROVIDER.—The term ''service provider'' means any person or entity, other than a platform operator, that processes or transfers covered data in the course of performing a service or function on behalf of, and at the direction of, a platform operator, an operator of an automated exposure notification service, or a public health authority, but only to the extent that such processing or transfer relates to the performance of such service or function.

(16) STATE.—The term ''State'' means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

(17) TRANSFER.—The term ''transfer'' means to disclose, release, share, disseminate, make available, allow access to, sell, license, or otherwise communicate covered data by any means to a non-affiliated entity or person.

SEC. 3. PUBLIC TRUST IN AUTOMATED EXPOSURE NOTIFICATION SERVICES.

(a) COLLABORATION WITH PUBLIC HEALTH.—An operator of an automated exposure notification service shall collaborate with a public health authority in the operation of such service.

(b) DIAGNOSIS INFORMATION.—An operator of an automated exposure notification service may not collect, process, or transfer an actual, potential, or presumptive positive diagnosis of an infectious disease as part of the automated exposure notification service, unless such diagnosis is an authorized diagnosis.

(c) ACCURACY AND RELIABILITY.—An operator of an automated exposure notification service shall publish—

(1) guidance for the public on the functionality of the service and how to interpret the notifications, including any limitation with respect to the accuracy or reliability of the exposure risk; and

(2) measures of the effectiveness of the service offered, including adoption rates.

(d) PREVENTION OF DECEPTIVE ACTS OR PRACTICES.—It shall be unlawful for a platform operator or an operator of an automated exposure notification service to engage in a deceptive act or practice concerning an automated exposure notification service.

(e) SERVICE PROVIDER REQUIREMENT.—When a service provider has actual knowledge that an operator of an automated exposure notification service or a public health authority has engaged in an act or practice that fails to adhere to the standards set forth in sections 3 through 8 of this Act, the service provider shall notify the automated exposure notification service or the public health authority, as applicable, of the potential violation or failure to adhere to such standards.

SEC. 4. VOLUNTARY PARTICIPATION AND TRANSPARENCY.

(a) VOLUNTARY PARTICIPATION.—

(1) ENROLLMENT WITH AFFIRMATIVE EXPRESS CONSENT.—An operator of an automated exposure notification service—

(A) may not enroll an individual in the automated exposure notification service without the individual's prior affirmative express consent; and

(B) shall provide an individual with a clear and conspicuous means to withdraw affirmative express consent to the individual's enrollment in the automated exposure notification service.

(2) RIGHT TO IDENTIFY A DIAGNOSIS.—An individual with an authorized diagnosis shall determine whether the individual's authorized diagnosis is

processed as part of the automated exposure notification service.

(b) NOTICE OF COVERED DATA PRACTICES.—An operator of an automated exposure notification service and a platform operator shall make publicly and persistently available, in a conspicuous and readily accessible manner, a privacy policy that provides a detailed and accurate representation of that person or entity's covered data collection, processing, and transfer activities in connection with such person or entity's automated exposure notification service or the facilitation of such service. Such privacy policy shall include, at a minimum—

(1) the identity and the contact information of the person or entity, including the contact information for the person or entity's representative for privacy and covered data security inquiries;

(2) each category of covered data the person or entity collects and the limited allowable processing purposes for which such covered data is collected in accordance with section 5;

(3) whether the person or entity transfers covered data for the limited allowable purposes in section 5 and, if so, a detailed description of the data transferred, the purpose of the transfer, and the identity of the recipient of the transfer;

(4) a description of the person or entity's covered data minimization and retention policies;

(5) how an individual can exercise the individual rights described in this title;

(6) a description of the person or entity's covered data security policies; and

(7) the effective date of the privacy policy.

(c) LANGUAGES.—A person or entity shall make the privacy policy required under this section available to the public in all of the languages in which the person or entity provides, or facilitates the provision of, an automated exposure notification service.

SEC. 5. DATA RESTRICTIONS.

(a) COLLECTION AND PROCESSING RESTRICTIONS.—An operator of an automated exposure notification service may not collect or process any covered data—

(1) beyond the minimum amount necessary to implement an automated exposure notification service for public health purposes; or

(2) for any commercial purpose.

(b) TRANSFER RESTRICTIONS.—An operator of an automated exposure notification service may not transfer any covered data, except—

(1) to provide notification of a potential exposure to an individual who has enrolled in the automated exposure notification service;

(2) to a public health authority for public health purposes related to an infectious disease;

(3) to its service provider, by contract, to—

(A) perform system maintenance, debug systems, or repair any error to ensure the functionality of the automated exposure notification service, provided such processing is limited to this purpose; or

(B) detect or respond to a security incident, provide a secure environment, or maintain the safety of the automated exposure notification service, provided such process is limited to this purpose; or

(4) to comply with the establishment, exercise, or defense of a legal claim.

(c) FURTHER RESTRICTIONS.—

(1) IN GENERAL.—It shall be unlawful for any person, entity, or Executive agency to transfer covered data to any Executive agency unless the information is transferred in connection with an investigation or enforcement proceeding under this Act.

(2) PROHIBITION.—An Executive agency may not process or transfer covered data, except—

(A) for a public health purpose related to an infectious disease; or

(B) in connection with an investigation or enforcement proceeding under this Act.

(d) RESEARCH.—This section shall not be construed to prohibit data collection, processing, or transfers to carry out research—

(1) conducted pursuant to the Federal policy for the protection of human subjects under part 46 of title 45, Code of Federal Regulations; or

(2) for the development, manufacture, or distribution of a drug, biological product, or vaccine that relates to an infectious disease conducted pursuant to part 50 of title 21, Code of Federal Regulations.

SEC. 6. DATA DELETION.

(a) DELETION UPON REQUEST.—Upon the request of an individual, an operator of an automated exposure notification service shall delete, or allow the individual to delete, all covered data of the individual that is processed by the operator.

(b) RECURRING DELETION.—An operator of an automated exposure notification service shall delete the covered

data of a participating individual within 30 days of receipt of such covered data, on a rolling basis, or at such times as is consistent with a standard published by a public health authority within an applicable jurisdiction.

(c) APPLICABILITY TO SERVICE PROVIDERS.—An operator of an automated exposure notification service shall instruct any service provider to which the entity transfers covered data to delete such data in accordance with the requirements of this subsection.

(d) RESEARCH.—This section shall not be construed to prohibit data retention for public health research purposes consistent with the requirements in section 5(d).

SEC. 7. DATA SECURITY.

(a) IN GENERAL.—An operator of an automated exposure notification service shall establish, implement, and maintain data security practices to protect the confidentiality, integrity, availability, and accessibility of covered data. Such covered data security practices shall be consistent with standards generally accepted by experts in the information security field.

(b) SPECIFIC REQUIREMENTS.—Covered data security practices required under subsection (a) shall include, at a minimum, the following:

(1) ASSESS RISKS AND VULNERABILITIES.—Identifying and assessing any reasonably foreseeable

risks to, and vulnerabilities in, each system maintained by the person or entity that processes or transfers covered data, including unauthorized access to or risks to covered data, human and technical vulnerabilities, access rights, and use of service providers. Such activities shall include a plan to receive and respond to unsolicited reports of risks and vulnerabilities by entities and individuals, developing and testing systems for monitoring the security of covered data, and resilience against denial of service attacks and malicious disinformation.

(2) PREVENTIVE AND CORRECTIVE ACTION.—Taking preventive and corrective action to mitigate any risks or vulnerabilities to covered data identified by the person or entity, which may include implementing administrative, technical, or physical safeguards or changes to covered data security practices or the architecture, installation, or implementation of network or operating software.

(3) BREACH NOTIFICATION.—Maintaining plans for responding to security incidents involving covered data and, in the most expedient time possible, consistent with the legitimate needs of law enforcement, notifying any individual whose data is subject to a security breach, as well as the Federal Trade Com-

mission, of the breach, the data involved, any reasonably foreseeable impacts of the breach for individuals whose data is subject to the breach, the steps individuals may take to mitigate those impacts, and the measures the operator of the automated exposure notification service is taking to prevent a future incident. An operator of an automated exposure notification service shall require its service providers to provide notice to the operator of the automated exposure notification service of any breach of the security of the covered data immediately following the discovery of the breach.

(c) INTERFERENCE PROHIBITED.—It shall be unlawful for any person or entity to transmit signals with the intent to cause an automated exposure notification service to produce inaccurate notifications or to otherwise interfere with the intended functioning of such a service.

SEC. 8. FREEDOM OF MOVEMENT AND NONDISCRIMINATION.

It shall be unlawful for any person or entity to segregate, discriminate against, or otherwise make unavailable to an individual or class of individuals the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation (as such term is defined in section 301 of the Americans With Disabilities

Act of 1990 (42 U.S.C. 12181)), based on covered data collected or processed through an automated exposure notification service or an individual's choice to use or not use an automated exposure notification service.

SEC. 9. OVERSIGHT.

(a) IN GENERAL.—Section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee) is amended—

(1) in subsection (c)—

(A) in paragraph (1), by inserting ''or to respond to health-related epidemics'' after ''from terrorism''; and

(B) in paragraph (2), by inserting ''or to respond to health-related epidemics'' after ''against terrorism''; and

(2) in subsection (d)—

(A) in paragraph (1), by inserting ''or to respond to health-related epidemics'' after ''from terrorism'' each place it appears; and

(B) in paragraph (2)—

(i) in subparagraph (B), by striking ''and'' at the end;

(ii) in subparagraph (C), by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

''(D) the collection, use, storage, and sharing of covered data by Federal, State, or local government in connection with responding to a Federal declaration of a public health emergency to ensure that privacy and civil liberties are protected.''.

(b) REPORTS.—Section 1061(e) of the Intelligence Reform and Terrorism Prevention Act of 2004 (42 U.S.C. 2000ee(e)) is amended by adding at the end the following:

''(3) REPORT ON COVID–19 MITIGATION ACTIVITIES.—Not later than 1 year after the date of enactment of this paragraph, the Board shall issue a report, which shall be publicly available to the greatest extent possible, assessing the impact on privacy and civil liberties of Government activities in response to the public health emergency related to the Coronavirus 2019 (COVID–19), and making recommendations for how the Government should mitigate the threats posed by such emergency.

''(4) REPORTS ON PUBLIC HEALTH EMERGENCY RESPONSE.—Not later than 1 year after any Federal emergency or disaster declaration related to public health, or not later than 1 year after the termination

of such declaration, the Board shall issue a report, which shall be publicly available to the greatest extent possible, assessing the impact on privacy and civil liberties of Government activities in response to such emergency or disaster, and making recommendations for how the Government should mitigate the threats posed by such emergency or disaster.''.

SEC. 10. ENFORCEMENT.

(a) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) POWERS OF THE COMMISSION.—

(A) IN GENERAL.—Except as provided in paragraphs (3) and (4) of this subsection, the Federal Trade Commission (referred to in this Act as 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.—Any person who violates this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

(C) EFFECT ON OTHER LAWS.—Nothing in this Act shall be construed to limit the authority of the Commission under any other provision of law.

(3) INDEPENDENT LITIGATION AUTHORITY.—Notwithstanding section 16 of the Federal Trade Commission Act (15 U.S.C. 56), the Commission may commence, defend, or intervene in, and supervise the litigation of, any civil action under this Act (including an action to collect a civil penalty) and any appeal of such action in its own name by any of its attorneys designated by it for such purpose. The Commission shall notify the Attorney General of any such action and may consult with the Attorney General with respect to any such action or request the Attorney General on behalf of the Commission to commence, defend, or intervene in any such action.

(4) NONPROFIT ORGANIZATIONS AND COMMUNICATIONS COMMON CARRIERS.—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 other jurisdictional limitation of the Commission, the Commission shall also enforce this Act in the same manner provided in paragraphs (1), (2), and (3) of this subsection, with respect to—

(A) any organization not organized to carry on business for the organization's own profit or that of the organization's members; and

(B) common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et 23 seq.) and all Acts amendatory thereof and supplementary thereto.

(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) IN GENERAL.—If the chief law enforcement officer of a State, or an official or agency designated by a State, has reason to believe that any person has violated or is violating this Act, the attorney general, official, or agency of the State, in addition to any authority it may have to bring an action in State court under its consumer protection law, may bring

a civil action in any appropriate United States district court or in any other court of competent jurisdiction, including a State court, to—

(A) enjoin further such violation by such person;

(B) enforce compliance with this Act;

(C) obtain civil penalties; and

(D) obtain damages, restitution, or other compensation on behalf of residents of the State.

(2) NOTICE AND INTERVENTION BY THE FTC.—The attorney general of a State shall provide prior written notice of any action under paragraph (1) to the Commission and provide the Commission with a copy of the complaint in the action, except in any case in which such prior notice is not feasible, in which case the attorney general shall serve such notice immediately upon instituting such action. The Commission shall have the right—

(A) to intervene in the action;

(B) upon so intervening, to be heard on all matters arising therein; and

(C) to file petitions for appeal.

(3) RELATIONSHIP WITH STATE LAW CLAIMS.—If the attorney general of a State has authority to

bring an action under State law directed at any act or practice that also violates this Act, the attorney general may assert the State law claim and a claim under this Act in the same civil action.

(c) STATE LAW PRESERVATION.—Nothing in this Act shall be construed to preempt, displace, or supplant any State law, rule, regulation, or requirement, including—

(1) any consumer protection law of general applicability such as any law regulating deceptive, unfair, or unconscionable practices;

(2) any health privacy or infectious disease law;

(3) any civil rights law;

(4) any law that governs the privacy rights or other protections of employees, employee information, or students or student information;

(5) any law that addresses notification requirements in the event of a covered data breach;

(6) contract or tort law;

(7) any criminal law governing fraud, theft, unauthorized access to information or unauthorized use of information, malicious behavior, and similar provisions, and any law of criminal procedure;

(8) any law specifying a remedy or a cause of action to an individual; or

(9) any public safety or sector-specific law unrelated to privacy or security.

(d) PRESERVATION OF COMMON LAW OR STATUTORY CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this Act, nor any amendment, standard, rule, requirement, assessment, law, or regulation promulgated under this Act, shall be construed to preempt, displace, or supplant any Federal or State common law right or remedy, or any statute creating a remedy for civil relief, including any cause of action for personal injury, wrongful death, property damage, or other financial, physical, reputational, or psychological injury based in negligence, strict liability, products liability, failure to warn, an objectively offensive intrusion into the private affairs or concerns of the individual, or any other legal theory of liability under any Federal or State common law, or any State statutory law.

(e) SEVERABILITY.—If any provision of this Act, or the application thereof to any person or entity or circumstance, is held invalid, the remainder of this Act and the application of such provision to other persons or entities not similarly situated or to other circumstances shall not be affected by the invalidation.

(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as are nec-

essary to carry out this Act and the amendments made by this Act.

(g) EFFECTIVE DATE.—This Act and the amendments made by this Act shall take effect on the date of the enactment of this Act.