

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.

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

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) **SHORT TITLE.**—This Act may be cited as the
5 “Exposure Notification Privacy Act”.

6 (b) **TABLE OF CONTENTS.**—The table of contents for
7 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.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) **AFFIRMATIVE EXPRESS CONSENT.**—

4 (A) **IN GENERAL.**—The term “affirmative
5 express consent” means an affirmative act by
6 an individual that clearly communicates the in-
7 dividual’s authorization for an act or practice,
8 in response to a specific request that—

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

13 (ii) includes a description of each act
14 or practice for which the individual’s con-
15 sent is sought and—

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

18 (II) includes a prominent heading
19 that would enable a reasonable indi-
20 vidual to identify and understand the
21 act or practice.

22 (B) **EXPRESS CONSENT REQUIRED.**—Af-
23 firmative express consent shall not be inferred

1 from the inaction of an individual or the indi-
2 vidual's continued use of a service or product.

3 (C) VOLUNTARY.—Affirmative express
4 consent shall be freely given and noncondi-
5 tioned.

6 (2) AGGREGATE DATA.—The term “aggregate
7 data” means information that relates to a group or
8 category of individuals that is not linked or reason-
9 ably linkable to any individual or device that is
10 linked or reasonably linkable to an individual, pro-
11 vided that a platform operator or operator of an
12 automated exposure notification service—

13 (A) takes reasonable measures to safe-
14 guard the data from reidentification;

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

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

21 (D) contractually requires the same com-
22 mitment for all transfers of the data.

23 (3) AUTHORIZED DIAGNOSIS.—The term “au-
24 thorized diagnosis” means an actual, potential, or
25 presumptive positive diagnosis of an infectious dis-

1 ease confirmed by a public health authority or a li-
2 censed health care provider.

3 (4) AUTOMATED EXPOSURE NOTIFICATION
4 SERVICE.—

5 (A) IN GENERAL.—The term “automated
6 exposure notification service” means a website,
7 online service, online application, mobile appli-
8 cation, or mobile operating system that is of-
9 fered in commerce in the United States and
10 that is designed, in part or in full, specifically
11 to be used for, or marketed for, the purpose of
12 digitally notifying, in an automated manner, an
13 individual who may have become exposed to an
14 infectious disease (or the device of such indi-
15 vidual, or a person or entity that reviews such
16 disclosures).

17 (B) LIMITATIONS.—Such term does not in-
18 clude—

19 (i) any technology that a public health
20 authority uses as a means to facilitate tra-
21 ditional in-person, email, or telephonic con-
22 tact tracing activities, or any similar tech-
23 nology that is used to assist individuals to
24 evaluate if they are experiencing symptoms
25 related to an infectious disease to the ex-

1 tent the technology is not used as an auto-
2 mated exposure notification service; or

3 (ii) any platform operator or service
4 provider that provides technology to facili-
5 tate an automated exposure notification
6 service to the extent the technology acts
7 only to facilitate such services and is not
8 itself used as an automated exposure noti-
9 fication service.

10 (5) COLLECT; COLLECTION.—The terms “col-
11 lect” and “collection” mean buying, renting, gath-
12 ering, obtaining, receiving, accessing, or otherwise
13 acquiring covered data by any means, including by
14 passively or actively observing the behavior of an in-
15 dividual.

16 (6) COVERED DATA.—The term “covered data”
17 means any information that is—

18 (A) linked or reasonably linkable to any in-
19 dividual or device linked or reasonably linkable
20 to an individual;

21 (B) not aggregate data; and

22 (C) collected, processed, or transferred in
23 connection with an automated exposure notifi-
24 cation service.

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

5 (8) DELETE.—The term “delete” means de-
6 stroying, permanently erasing, or otherwise modi-
7 fying covered data to make such covered data per-
8 manently unreadable or indecipherable and unre-
9 coverable.

10 (9) EXECUTIVE AGENCY.—The term “Executive
11 agency” has the meaning given such term in section
12 105 of title 5, United States Code.

13 (10) INDIAN TRIBE.—The term “Indian
14 tribe”—

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

19 (B) includes a Native Hawaiian organiza-
20 tion as defined in section 6207 of the Elemen-
21 tary and Secondary Education Act of 1965 (20
22 U.S.C. 7517).

23 (11) OPERATOR OF AN AUTOMATED EXPOSURE
24 NOTIFICATION SERVICE.—The term “operator of an
25 automated exposure notification service” means any

1 person or entity that operates an automated expo-
2 sure notification service, other than a public health
3 authority, and that is—

4 (A) subject to the Federal Trade Commis-
5 sion Act (15 U.S.C. 41 et seq.); or

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

7 (12) PLATFORM OPERATOR.—The term “plat-
8 form operator” means any person or entity other
9 than a service provider who provides an operating
10 system that includes features supportive of an auto-
11 mated exposure notification service and facilitates
12 the use or distribution of such automated exposure
13 notification service to the extent the technology is
14 not used by the platform operator as an automated
15 exposure notification service.

16 (13) PROCESS.—The term “process” means
17 any operation or set of operations performed on cov-
18 ered data, including collection, analysis, organiza-
19 tion, structuring, retaining, using, securing, or oth-
20 erwise handling covered data.

21 (14) PUBLIC HEALTH AUTHORITY.—The term
22 “public health authority” means an agency or au-
23 thority of the United States, a State, a territory, a
24 political subdivision of a State or territory, or an In-
25 dian tribe that is responsible for public health mat-

1 ters as part of its official mandate, or a person or
2 entity acting under a grant of authority from or con-
3 tract with such public agency.

4 (15) SERVICE PROVIDER.—The term “service
5 provider” means any person or entity, other than a
6 platform operator, that processes or transfers cov-
7 ered data in the course of performing a service or
8 function on behalf of, and at the direction of, a plat-
9 form operator, an operator of an automated expo-
10 sure notification service, or a public health author-
11 ity, but only to the extent that such processing or
12 transfer relates to the performance of such service
13 or function.

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

19 (17) TRANSFER.—The term “transfer” means
20 to disclose, release, share, disseminate, make avail-
21 able, allow access to, sell, license, or otherwise com-
22 municate covered data by any means to a non-
23 affiliated entity or person.

1 **SEC. 3. PUBLIC TRUST IN AUTOMATED EXPOSURE NOTIFI-**
2 **CATION SERVICES.**

3 (a) COLLABORATION WITH PUBLIC HEALTH.—An
4 operator of an automated exposure notification service
5 shall collaborate with a public health authority in the oper-
6 ation of such service.

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

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

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

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

21 (d) PREVENTION OF DECEPTIVE ACTS OR PRAC-
22 TICES.—It shall be unlawful for a platform operator or
23 an operator of an automated exposure notification service
24 to engage in a deceptive act or practice concerning an
25 automated exposure notification service.

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

10 **SEC. 4. VOLUNTARY PARTICIPATION AND TRANSPARENCY.**

11 (a) VOLUNTARY PARTICIPATION.—

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

15 (A) may not enroll an individual in the
16 automated exposure notification service without
17 the individual's prior affirmative express con-
18 sent; and

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

23 (2) RIGHT TO IDENTIFY A DIAGNOSIS.—An in-
24 dividual with an authorized diagnosis shall deter-
25 mine whether the individual's authorized diagnosis is

1 processed as part of the automated exposure notifi-
2 cation service.

3 (b) NOTICE OF COVERED DATA PRACTICES.—An op-
4 erator of an automated exposure notification service and
5 a platform operator shall make publicly and persistently
6 available, in a conspicuous and readily accessible manner,
7 a privacy policy that provides a detailed and accurate rep-
8 resentation of that person or entity’s covered data collec-
9 tion, processing, and transfer activities in connection with
10 such person or entity’s automated exposure notification
11 service or the facilitation of such service. Such privacy pol-
12 icy shall include, at a minimum—

13 (1) the identity and the contact information of
14 the person or entity, including the contact informa-
15 tion for the person or entity’s representative for pri-
16 vacy and covered data security inquiries;

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

21 (3) whether the person or entity transfers cov-
22 ered data for the limited allowable purposes in sec-
23 tion 5 and, if so, a detailed description of the data
24 transferred, the purpose of the transfer, and the
25 identity of the recipient of the transfer;

1 (4) a description of the person or entity's cov-
2 ered data minimization and retention policies;

3 (5) how an individual can exercise the indi-
4 vidual rights described in this title;

5 (6) a description of the person or entity's cov-
6 ered data security policies; and

7 (7) the effective date of the privacy policy.

8 (c) LANGUAGES.—A person or entity shall make the
9 privacy policy required under this section available to the
10 public in all of the languages in which the person or entity
11 provides, or facilitates the provision of, an automated ex-
12 posure notification service.

13 **SEC. 5. DATA RESTRICTIONS.**

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

17 (1) beyond the minimum amount necessary to
18 implement an automated exposure notification serv-
19 ice for public health purposes; or

20 (2) for any commercial purpose.

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

1 (1) to provide notification of a potential expo-
2 sure to an individual who has enrolled in the auto-
3 mated exposure notification service;

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

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

7 (A) perform system maintenance, debug
8 systems, or repair any error to ensure the
9 functionality of the automated exposure notifi-
10 cation service, provided such processing is lim-
11 ited to this purpose; or

12 (B) detect or respond to a security inci-
13 dent, provide a secure environment, or maintain
14 the safety of the automated exposure notifica-
15 tion service, provided such process is limited to
16 this purpose; or

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

19 (c) FURTHER RESTRICTIONS.—

20 (1) IN GENERAL.—It shall be unlawful for any
21 person, entity, or Executive agency to transfer cov-
22 ered data to any Executive agency unless the infor-
23 mation is transferred in connection with an inves-
24 tigation or enforcement proceeding under this Act.

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

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

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

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

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

13 (2) for the development, manufacture, or dis-
14 tribution of a drug, biological product, or vaccine
15 that relates to an infectious disease conducted pur-
16 suant to part 50 of title 21, Code of Federal Regula-
17 tions.

18 **SEC. 6. DATA DELETION.**

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

24 (b) RECURRING DELETION.—An operator of an auto-
25 mated exposure notification service shall delete the covered

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

5 (c) **APPLICABILITY TO SERVICE PROVIDERS.**—An op-
6 erator of an automated exposure notification service shall
7 instruct any service provider to which the entity transfers
8 covered data to delete such data in accordance with the
9 requirements of this subsection.

10 (d) **RESEARCH.**—This section shall not be construed
11 to prohibit data retention for public health research pur-
12 poses consistent with the requirements in section 5(d).

13 **SEC. 7. DATA SECURITY.**

14 (a) **IN GENERAL.**—An operator of an automated ex-
15 posure notification service shall establish, implement, and
16 maintain data security practices to protect the confiden-
17 tiality, integrity, availability, and accessibility of covered
18 data. Such covered data security practices shall be con-
19 sistent with standards generally accepted by experts in the
20 information security field.

21 (b) **SPECIFIC REQUIREMENTS.**—Covered data secu-
22 rity practices required under subsection (a) shall include,
23 at a minimum, the following:

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

1 risks to, and vulnerabilities in, each system main-
2 tained by the person or entity that processes or
3 transfers covered data, including unauthorized ac-
4 cess to or risks to covered data, human and tech-
5 nical vulnerabilities, access rights, and use of service
6 providers. Such activities shall include a plan to re-
7 ceive and respond to unsolicited reports of risks and
8 vulnerabilities by entities and individuals, developing
9 and testing systems for monitoring the security of
10 covered data, and resilience against denial of service
11 attacks and malicious disinformation.

12 (2) PREVENTIVE AND CORRECTIVE ACTION.—
13 Taking preventive and corrective action to mitigate
14 any risks or vulnerabilities to covered data identified
15 by the person or entity, which may include imple-
16 menting administrative, technical, or physical safe-
17 guards or changes to covered data security practices
18 or the architecture, installation, or implementation
19 of network or operating software.

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

1 mission, of the breach, the data involved, any rea-
2 sonably foreseeable impacts of the breach for indi-
3 viduals whose data is subject to the breach, the steps
4 individuals may take to mitigate those impacts, and
5 the measures the operator of the automated expo-
6 sure notification service is taking to prevent a future
7 incident. An operator of an automated exposure no-
8 tification service shall require its service providers to
9 provide notice to the operator of the automated ex-
10 posure notification service of any breach of the secu-
11 rity of the covered data immediately following the
12 discovery of the breach.

13 (c) INTERFERENCE PROHIBITED.—It shall be unlaw-
14 ful for any person or entity to transmit signals with the
15 intent to cause an automated exposure notification service
16 to produce inaccurate notifications or to otherwise inter-
17 fere with the intended functioning of such a service.

18 **SEC. 8. FREEDOM OF MOVEMENT AND NONDISCRIMINA-**
19 **TION.**

20 It shall be unlawful for any person or entity to seg-
21 regate, discriminate against, or otherwise make unavail-
22 able to an individual or class of individuals the goods, serv-
23 ices, facilities, privileges, advantages, or accommodations
24 of any place of public accommodation (as such term is de-
25 fined in section 301 of the Americans With Disabilities

1 Act of 1990 (42 U.S.C. 12181)), based on covered data
2 collected or processed through an automated exposure no-
3 tification service or an individual’s choice to use or not
4 use an automated exposure notification service.

5 **SEC. 9. OVERSIGHT.**

6 (a) IN GENERAL.—Section 1061 of the Intelligence
7 Reform and Terrorism Prevention Act of 2004 (42 U.S.C.
8 2000ee) is amended—

9 (1) in subsection (c)—

10 (A) in paragraph (1), by inserting “or to
11 respond to health-related epidemics” after
12 “from terrorism”; and

13 (B) in paragraph (2), by inserting “or to
14 respond to health-related epidemics” after
15 “against terrorism”; and

16 (2) in subsection (d)—

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

20 (B) in paragraph (2)—

21 (i) in subparagraph (B), by striking
22 “and” at the end;

23 (ii) in subparagraph (C), by striking
24 the period at the end and inserting “;
25 and”; and

1 (iii) by adding at the end the fol-
2 lowing:

3 “(D) the collection, use, storage, and shar-
4 ing of covered data by Federal, State, or local
5 government in connection with responding to a
6 Federal declaration of a public health emer-
7 gency to ensure that privacy and civil liberties
8 are protected.”.

9 (b) REPORTS.—Section 1061(e) of the Intelligence
10 Reform and Terrorism Prevention Act of 2004 (42 U.S.C.
11 2000ee(e)) is amended by adding at the end the following:

12 “(3) REPORT ON COVID–19 MITIGATION ACTIVI-
13 TIES.—Not later than 1 year after the date of enact-
14 ment of this paragraph, the Board shall issue a re-
15 port, which shall be publicly available to the greatest
16 extent possible, assessing the impact on privacy and
17 civil liberties of Government activities in response to
18 the public health emergency related to the
19 Coronavirus 2019 (COVID–19), and making rec-
20 ommendations for how the Government should miti-
21 gate the threats posed by such emergency.

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

1 of such declaration, the Board shall issue a report,
2 which shall be publicly available to the greatest ex-
3 tent possible, assessing the impact on privacy and
4 civil liberties of Government activities in response to
5 such emergency or disaster, and making rec-
6 ommendations for how the Government should miti-
7 gate the threats posed by such emergency or dis-
8 aster.”.

9 **SEC. 10. ENFORCEMENT.**

10 (a) ENFORCEMENT BY THE FEDERAL TRADE COM-
11 MISSION.—

12 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
13 TICES.—A violation of this Act shall be treated as
14 a violation of a rule defining an unfair or deceptive
15 act or practice prescribed under section 18(a)(1)(B)
16 of the Federal Trade Commission Act (15 U.S.C.
17 57a(a)(1)(B)).

18 (2) POWERS OF THE COMMISSION.—

19 (A) IN GENERAL.—Except as provided in
20 paragraphs (3) and (4) of this subsection, the
21 Federal Trade Commission (referred to in this
22 Act as the “Commission”) shall enforce this Act
23 in the same manner, by the same means, and
24 with the same jurisdiction, powers, and duties
25 as though all applicable terms and provisions of

1 the Federal Trade Commission Act (15 U.S.C.
2 41 et seq.) were incorporated into and made a
3 part of this Act.

4 (B) PRIVILEGES AND IMMUNITIES.—Any
5 person who violates this Act shall be subject to
6 the penalties and entitled to the privileges and
7 immunities provided in the Federal Trade Com-
8 mission Act.

9 (C) EFFECT ON OTHER LAWS.—Nothing in
10 this Act shall be construed to limit the author-
11 ity of the Commission under any other provi-
12 sion of law.

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

1 (4) NONPROFIT ORGANIZATIONS AND COMMU-
2 NICATIONS COMMON CARRIERS.—Notwithstanding
3 section 4, 5(a)(2), or 6 of the Federal Trade Com-
4 mission Act (15 U.S.C. 44, 45(a)(2), 46) or any
5 other jurisdictional limitation of the Commission, the
6 Commission shall also enforce this Act in the same
7 manner provided in paragraphs (1), (2), and (3) of
8 this subsection, with respect to—

9 (A) any organization not organized to
10 carry on business for the organization’s own
11 profit or that of the organization’s members;
12 and

13 (B) common carriers subject to the Com-
14 munications Act of 1934 (47 U.S.C. 151 et 23
15 seq.) and all Acts amendatory thereof and sup-
16 plementary thereto.

17 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-
18 ERAL.—

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

1 a civil action in any appropriate United States dis-
2 trict court or in any other court of competent juris-
3 diction, including a State court, to—

4 (A) enjoin further such violation by such
5 person;

6 (B) enforce compliance with this Act;

7 (C) obtain civil penalties; and

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

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

20 (A) to intervene in the action;

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

23 (C) to file petitions for appeal.

24 (3) RELATIONSHIP WITH STATE LAW CLAIMS.—

25 If the attorney general of a State has authority to

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

5 (c) STATE LAW PRESERVATION.—Nothing in this
6 Act shall be construed to preempt, displace, or supplant
7 any State law, rule, regulation, or requirement, includ-
8 ing—

9 (1) any consumer protection law of general ap-
10 plicability such as any law regulating deceptive, un-
11 fair, or unconscionable practices;

12 (2) any health privacy or infectious disease law;

13 (3) any civil rights law;

14 (4) any law that governs the privacy rights or
15 other protections of employees, employee informa-
16 tion, or students or student information;

17 (5) any law that addresses notification require-
18 ments in the event of a covered data breach;

19 (6) contract or tort law;

20 (7) any criminal law governing fraud, theft, un-
21 authorized access to information or unauthorized use
22 of information, malicious behavior, and similar pro-
23 visions, and any law of criminal procedure;

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

1 (9) any public safety or sector-specific law unre-
2 lated to privacy or security.

3 (d) PRESERVATION OF COMMON LAW OR STATUTORY
4 CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this
5 Act, nor any amendment, standard, rule, requirement, as-
6 sessment, law, or regulation promulgated under this Act,
7 shall be construed to preempt, displace, or supplant any
8 Federal or State common law right or remedy, or any stat-
9 ute creating a remedy for civil relief, including any cause
10 of action for personal injury, wrongful death, property
11 damage, or other financial, physical, reputational, or psy-
12 chological injury based in negligence, strict liability, prod-
13 ucts liability, failure to warn, an objectively offensive in-
14 trusion into the private affairs or concerns of the indi-
15 vidual, or any other legal theory of liability under any Fed-
16 eral or State common law, or any State statutory law.

17 (e) SEVERABILITY.—If any provision of this Act, or
18 the application thereof to any person or entity or cir-
19 cumstance, is held invalid, the remainder of this Act and
20 the application of such provision to other persons or enti-
21 ties not similarly situated or to other circumstances shall
22 not be affected by the invalidation.

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

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

3 (g) **EFFECTIVE DATE.**—This Act and the amend-
4 ments made by this Act shall take effect on the date of
5 the enactment of this Act.