

118TH CONGRESS
1ST SESSION

S. 3337

To establish national data privacy standards in the United States, and for other purposes.

IN THE SENATE OF THE UNITED STATES

NOVEMBER 15, 2023

Ms. CORTEZ MASTO introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To establish national data privacy standards in the United States, and for other purposes.

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.**

4 This Act may be cited as the “Digital Accountability
5 and Transparency to Advance Privacy Act” or the “DATA
6 Privacy Act”.

7 **SEC. 2. DEFINITIONS.**

8 (a) IN GENERAL.—In this Act:

9 (1) COLLECT.—The term “collect” means tak-
10 ing any operation or set of operations to obtain cov-

1 ered data, including by automated means, including
2 purchasing, leasing, assembling, recording, gath-
3 ering, acquiring, or procuring.

4 (2) COMMISSION.—The term “Commission”
5 means the Federal Trade Commission.

6 (3) COVERED DATA.—The term “covered
7 data”—

8 (A) means any information that is—

9 (i) collected, processed, stored, or dis-
10 closed by a covered entity;

11 (ii) collected over the internet or other
12 digital network; and

13 (iii)(I) linked to an individual or de-
14 vice associated with an individual; or

15 (II) practicably linkable to an indi-
16 vidual or device associated with an indi-
17 vidual, including by combination with sepa-
18 rate information, by the covered entity or
19 any potential recipient of the data; and

20 (B) does not include data that is—

21 (i) collected, processed, stored, or dis-
22 closed solely for the purpose of employ-
23 ment of an individual; or

1 (ii) lawfully made available to the
2 public from Federal, State, or local govern-
3 ment records.

4 (4) COVERED ENTITY.—The term “covered en-
5 tity”—

6 (A) means any entity that collects, proc-
7 esses, stores, or discloses covered data; and

8 (B) does not include any entity that col-
9 lects, processes, stores, or discloses covered data
10 relating to fewer than 50,000 individuals and
11 devices during any 12-month period.

12 (5) DISCLOSE.—The term “disclose” means
13 taking any action with respect to covered data, in-
14 cluding by automated means, to sell, share, provide,
15 or otherwise transfer covered data to another entity,
16 person, or the general public.

17 (6) PRIVACY ENHANCING TECHNOLOGY.—The
18 term “privacy enhancing technology” means any—

19 (A) software solution, technical processes,
20 or other technological means of enhancing the
21 privacy and confidentiality of an individual’s
22 covered data in data or sets of data; or

23 (B) de-identification, anonymization, or
24 pseudonymization technologies or techniques,
25 filtering tools, anti-tracking technology, dif-

1 ferential privacy tools, synthetic data generation
2 tools, cryptographic techniques (such as secure
3 multi-party computation and homomorphic
4 encryption), or systems for federated learning.

5 (7) PRIVACY RISK.—The term “privacy risk”
6 means potential harm to an individual resulting
7 from the collection, processing, storage, or disclosure
8 of covered data, including—

- 9 (A) direct or indirect financial loss;
10 (B) stigmatization or reputational harm;
11 (C) anxiety, embarrassment, fear, and
12 other severe emotional trauma;
13 (D) loss of economic opportunity; or
14 (E) physical harm.

15 (8) PROCESS.—The term “process” means any
16 operation or set of operations that is performed on
17 covered data or on sets of covered data, including by
18 automated means, including organizing, combining,
19 adapting, altering, using, or transforming.

20 (9) PROTECTED CHARACTERISTIC.—The term
21 “protected characteristic” means an individual’s
22 race, sex, gender, sexual orientation, nationality, re-
23 ligious belief, age, or disability status.

24 (10) PSEUDONYMOUS DATA.—The term “pseu-
25 donymous data” means covered data that may only

1 be linked to the identity of an individual or the iden-
2 tity of a device associated with an individual if com-
3 bined with separate information.

4 (11) REASONABLE INTEREST.—The term “rea-
5 sonable interest” means—

6 (A) a compelling business, operational, ad-
7 ministrative, legal, or educational justification
8 for the collection, processing, storage, or disclo-
9 sure of covered data exists; and

10 (B) the interest does not subject the indi-
11 vidual linked to the covered data to an unrea-
12 sonable privacy risk.

13 (12) SENSITIVE DATA.—The term “sensitive
14 data” means any covered data relating to—

15 (A) the health, biologic, physiologic, bio-
16 metric, sexual life, or genetic information of an
17 individual; or

18 (B) the precise geolocation information of
19 a device associated with an individual.

20 (13) STORE.—The term “store” means any op-
21 eration or set of operations to continue possession of
22 covered data, including by automated means.

23 (14) THIRD PARTY SERVICE PROVIDER.—The
24 term “third party service provider” means any cov-
25 ered entity that collects, processes, stores, or dis-

1 closes covered data at the direction of, and for the
2 sole benefit of, another covered entity under a con-
3 tract.

4 (b) **MODIFIED DEFINITION BY RULEMAKING.**—If the
5 Commission determines that a term defined in paragraph
6 (10) or (12) is not sufficient to protect an individual’s
7 data privacy, the Commission may promulgated regula-
8 tions under section 553 of title 5, United States Code,
9 to modify the definition as the Commission considers ap-
10 propriate.

11 **SEC. 3. REQUIRED PRIVACY NOTICE.**

12 (a) **PRIVACY NOTICE.**—Each covered entity shall post
13 in an accessible location a notice that is concise, in con-
14 text, in easily understandable language, accurate, clear,
15 timely, updated, uses visualizations where appropriate,
16 conspicuous, and free of charge regarding the covered en-
17 tity’s privacy practices.

18 (b) **CONTENTS OF NOTICE.**—The notice required by
19 subsection (a) shall include—

20 (1) a description of the covered data that the
21 entity collects, processes, stores, and discloses, in-
22 cluding the sources that provided the covered data if
23 the covered entity did not collect the covered data
24 from the individual;

1 (2) the purposes for and means by which the
2 entity collects, processes, and stores the covered
3 data;

4 (3) the persons and entities to whom, and pur-
5 poses for which, the covered entity discloses the cov-
6 ered data; and

7 (4) a conspicuous, clear, and understandable
8 means for individuals to access the methods nec-
9 essary to exercise their rights under sections 4 and
10 5.

11 **SEC. 4. REQUIRED DATA PRACTICES.**

12 (a) REGULATIONS.—Not later than 1 year after the
13 date of the enactment of this Act, the Commission shall
14 promulgate regulations under section 553 of title 5,
15 United States Code, that require covered entities to imple-
16 ment, practice, and maintain certain data procedures and
17 processes that meet the following requirements:

18 (1) MINIMUM DATA PROCESSING REQUIRE-
19 MENTS.—Except as provided in subsection (b), re-
20 quire covered entities to meet all of the following re-
21 quirements regarding the means by and purposes for
22 which covered data is collected, processed, stored,
23 and disclosed:

24 (A) REASONABLE.—

1 (i) IN GENERAL.—Except as provided
2 in paragraph (3), covered data collection,
3 processing, storage, and disclosure prac-
4 tices must meet a reasonable interest of
5 the covered entity, including—

6 (I) business, educational, and ad-
7 ministrative operations that are rel-
8 evant and appropriate to the context
9 of the relationship between the cov-
10 ered entity and the individual linked
11 to the covered data;

12 (II) relevant and appropriate
13 product and service development and
14 enhancement;

15 (III) preventing and detecting
16 abuse, fraud, and other criminal activ-
17 ity;

18 (IV) reasonable communications
19 and marketing practices that follow
20 best practices, rules, and ethical
21 standards;

22 (V) engaging in scientific, med-
23 ical, or statistical research that fol-
24 lows commonly accepted ethical stand-
25 ards; or

1 (VI) any other purpose for which
2 the Commission considers to be rea-
3 sonable.

4 (ii) CONSIDERATIONS.—In promul-
5 gating regulations in accordance with this
6 subparagraph, the Commission shall con-
7 sider—

8 (I) the role of impact assess-
9 ments in determining the privacy risk
10 for high risk processing;

11 (II) the sensitivity of the covered
12 data; and

13 (III) the impact of such regula-
14 tions on small business.

15 (B) EQUITABLE.—

16 (i) IN GENERAL.—Covered data col-
17 lection, processing, storage, and disclosure
18 practices may not be for purposes that re-
19 sult in discrimination against a protected
20 characteristic, including—

21 (I) discriminatory targeted adver-
22 tising practices;

23 (II) price, service, or employment
24 opportunity discrimination; or

1 (III) any other practice the Com-
2 mission considers likely to result in
3 discrimination against a protected
4 characteristic.

5 (ii) CONSIDERATIONS.—In promul-
6 gating regulations in accordance with this
7 subparagraph, the Commission shall con-
8 sider—

9 (I) established civil rights laws,
10 common law, and existing relevant
11 consent decrees;

12 (II) the existing economic models
13 and technology available in the digital
14 advertising system;

15 (III) the role of algorithms and
16 impact assessments; and

17 (IV) the impact of such regula-
18 tions on small businesses.

19 (C) FORTHRIGHT.—

20 (i) IN GENERAL.—Covered data col-
21 lection, processing, storage, and disclosure
22 practices may not be accomplished with
23 means or for purposes that are deceptive,
24 including—

1 (I) the use of inconspicuous re-
2 cording or tracking devices and meth-
3 ods;

4 (II) the disclosure of covered
5 data that a reasonable individual be-
6 lieves to be the content of a private
7 communication with another party or
8 parties;

9 (III) notices, interfaces, or other
10 representations likely to mislead con-
11 sumers; or

12 (IV) any other practice that the
13 Commission considers likely to mis-
14 lead individuals regarding the pur-
15 poses for and means by which covered
16 data is collected, processed, stored, or
17 disclosed.

18 (ii) CONSIDERATIONS.—In promul-
19 gating regulations in accordance with this
20 subparagraph, the Commission shall con-
21 sider—

22 (I) existing relevant consent de-
23 crees;

24 (II) the reasonable expectations
25 of consumers;

- 1 (III) research on deceptive prac-
2 tices;
3 (IV) the role of deceptive user
4 interfaces; and
5 (V) the impact of such regula-
6 tions on small businesses.

7 (2) REQUIREMENTS FOR OPT-OUT CONSENT.—
8 Except as provided in subsection (b), require covered
9 entities to provide individuals with conspicuous ac-
10 cess to a method that is in easily understandable
11 language, concise, accurate, clear, to opt-out of any
12 collection, processing, storage, or disclosure of cov-
13 ered data linked to the individual.

14 (3) REQUIREMENTS FOR AFFIRMATIVE CON-
15 SENT.—Except as provided in subsection (b), require
16 covered entities to provide individuals with a notice
17 that is concise, in easily understandable language,
18 accurate, clear, timely, and conspicuous to express
19 affirmative, opt in consent—

20 (A) before the covered entity collects or
21 discloses sensitive data linked to the individual;
22 or

23 (B) before the covered entity collects, proc-
24 esses, stores, or discloses data for purposes
25 which are outside the context of the relationship

1 of the covered entity with the individual linked
2 to the data, including—

3 (i) the use of covered data beyond
4 what is necessary to provide, improve, or
5 market a good or service that the indi-
6 vidual requests;

7 (ii) the processing or disclosure of
8 covered data differs in material ways from
9 the purposes described in the privacy pol-
10 icy that was in effect when the data was
11 collected;

12 (iii) any other purpose that Commis-
13 sion considers outside of context.

14 (4) DATA MINIMIZATION REQUIREMENTS.—Ex-
15 cept as provided in subsection (b), require covered
16 entities to—

17 (A) take reasonable measures to limit the
18 collection, processing, storage, and disclosure of
19 covered data to the amount that is necessary to
20 carry out the purposes for which the data is col-
21 lected; and

22 (B) store covered data only as long as is
23 reasonably necessary to carry out the purposes
24 for which the data was collected.

1 (b) EXEMPTIONS.—Subsection (a) shall not apply if
2 the limitations on the collection, processing, storage, or
3 disclosure of covered data would—

4 (1) inhibit detection or prevention of a security
5 risk or incident;

6 (2) risk the health, safety, or property of the
7 covered entity or individual; or

8 (3) prevent compliance with an applicable law
9 (including regulations) or legal process.

10 **SEC. 5. INDIVIDUAL CONTROL OVER DATA USE.**

11 (a) REGULATIONS.—Not later than 1 year after the
12 date of the enactment of this Act, the Commission shall
13 promulgate regulations under section 553 of title 5,
14 United States Code, to require covered entities to provide
15 conspicuous, understandable, clear, and free of charge
16 method to—

17 (1) upon the request of an individual, provide
18 the individual with access to, or an accurate rep-
19 resentation of, covered data linked to with the indi-
20 vidual or the individual’s device stored by the cov-
21 ered entity;

22 (2) upon the request of an individual, provide
23 the individual with a means to dispute and resolve
24 the accuracy or completeness of the covered data

1 linked to the individual or the individual's device
2 stored by the entity;

3 (3) upon the request of an individual, delete
4 any covered data that the covered entity stores
5 linked to the individual or the individual's device;
6 and

7 (4) when technically feasible, upon the request
8 of an individual, allow the individual to transmit or
9 transfer covered data linked to the individual or the
10 individual's device that is maintained by the entity
11 to the individual in a format that is standardized
12 and interoperable.

13 (b) PSEUDONYMOUS DATA.—If the covered data that
14 an individual has requested processed under subsection (a)
15 is pseudonymous data, a covered entity may decline the
16 request if processing the request is not technically feasible.

17 (c) TIMELINESS OF REQUESTS.—In fulfilling any re-
18 quests made by the individual under subsection (a) the
19 covered entity shall act in as timely a manner as is reason-
20 ably possible.

21 (d) ACCESS TO SAME SERVICE.—A covered entity
22 shall not discriminate against an individual because of any
23 action the individual took under their rights described in
24 subsection (a), including—

25 (1) denying goods or services to the individual;

1 (2) charging, or advertising, different prices or
2 rates for goods or services; or

3 (3) providing different quality of goods or serv-
4 ices.

5 (e) CONSIDERATION.—The Commission shall allow a
6 covered entity, by contract, to provide relevant obligations
7 to the individual under subsection (a) on behalf of a third
8 party service provider that collects, processes, stores, or
9 discloses covered data only on behalf of the covered entity.

10 **SEC. 6. INFORMATION SECURITY STANDARDS.**

11 (a) REQUIRED DATA SECURITY PRACTICES.—

12 (1) REGULATIONS.—Not later than 1 year after
13 the date of enactment of this Act, the Commission
14 shall promulgate regulations under section 553 of
15 title 5, United States Code, to require covered enti-
16 ties to establish and implement policies and proce-
17 dures regarding information security practices for
18 the treatment and protection of covered data taking
19 into consideration—

20 (A) the level of identifiability of the cov-
21 ered data and the associated privacy risk;

22 (B) the sensitivity of the covered data col-
23 lected, processed, and stored and the associated
24 privacy risk; and

1 (C) the currently available and widely ac-
2 cepted technological, administrative, and phys-
3 ical means to protect covered data under the
4 control of the covered entity;

5 (D) the cost associated with implementing,
6 maintaining, and regularly reviewing the safe-
7 guards; and

8 (E) the impact of these requirements on
9 small and medium sized businesses.

10 (2) LIMITATIONS.—In promulgating the regula-
11 tions required under this section, the Commission
12 shall consider a covered entity who is in compliance
13 with existing information security laws that the
14 Commission determines are sufficiently rigorous to
15 be in compliance with this section with respect to
16 particular types of covered data to the extent those
17 types of covered data are covered by such law, in-
18 cluding the following:

19 (A) Title V of the Gramm-Leach-Bliley Act
20 (15 U.S.C. 6801 et seq.).

21 (B) The Health Information Technology
22 for Economic and Clinical Health Act (42
23 U.S.C. 17931).

1 (C) The Health Insurance Portability and
2 Accountability Act of 1996 Security Rule (45
3 CFR 160.103 and part 164).

4 (D) Any other existing law requiring a cov-
5 ered entity to implement and maintain informa-
6 tion security practices and procedures that the
7 Commission determines to be sufficiently rig-
8 orous.

9 **SEC. 7. PRIVACY PROTECTION OFFICERS.**

10 (a) APPOINTMENT OF A PRIVACY PROTECTION OFFI-
11 CER.—Each covered entity with annual revenue in excess
12 of \$50,000,000 the prior year shall designate at least 1
13 appropriately qualified employee as a privacy protection
14 officer who shall—

15 (1) educate employees about compliance re-
16 quirements;

17 (2) train employees involved in data processing;

18 (3) conduct regular, comprehensive audits to
19 ensure compliance and make records of the audits
20 available to enforcement authorities upon request;

21 (4) maintain updated, clear, and understand-
22 able records of all data security practices undertaken
23 by the covered entity;

24 (5) serve as the point of contact between the
25 covered entity and enforcement authorities; and

1 (6) advocate for policies and practices within
2 the covered entity that promote individual privacy.

3 (b) PROTECTIONS.—The privacy protection officer
4 shall not be dismissed or otherwise penalized by the cov-
5 ered entity for performing any of the tasks assigned to
6 the person under this section.

7 **SEC. 8. RESEARCH INTO PRIVACY ENHANCING TECH-**
8 **NOLOGY.**

9 (a) NATIONAL SCIENCE FOUNDATION SUPPORT OF
10 RESEARCH ON PRIVACY ENHANCING TECHNOLOGY.—The
11 Director of the National Science Foundation, in consulta-
12 tion with other relevant Federal agencies (as determined
13 by the Director), shall support merit-reviewed and com-
14 petitively awarded research on privacy enhancing tech-
15 nologies, which may include—

16 (1) fundamental research on technologies for
17 de-identification, pseudonymization, anonymization,
18 or obfuscation to protect individuals' privacy in data
19 sets;

20 (2) fundamental research on algorithms, ma-
21 chine learning, and other computational processes or
22 tools used to protect individual privacy when col-
23 lecting, storing, sharing, aggregating, or analyzing
24 data;

1 (3) fundamental research on technologies that
2 promote data minimization principles in data collec-
3 tion, sharing, transfers, retention, and analytics;

4 (4) research awards on privacy enhancing tech-
5 nologies coordinated with other relevant Federal
6 agencies and programs;

7 (5) research on barriers to, and opportunities
8 for, the adoption of privacy enhancing technologies,
9 including studies on effective business models for
10 privacy enhancing technologies; and

11 (6) international cooperative research, awards,
12 challenges, and pilot projects on privacy enhancing
13 technologies with key allies and partners of the
14 United States.

15 (b) INTEGRATION INTO THE COMPUTER AND NET-
16 WORK SECURITY PROGRAM.—Subparagraph (D) of sec-
17 tion 4(a)(1) of the Cyber Security Research and Develop-
18 ment Act (15 U.S.C. 7403(a)(1)(D)) is amended to read
19 as follows:

20 “(D) privacy enhancing technologies and
21 confidentiality;”.

22 (c) COORDINATION WITH THE NATIONAL INSTITUTE
23 OF STANDARDS AND TECHNOLOGY AND OTHER STAKE-
24 HOLDERS.—

1 (1) IN GENERAL.—The Director of the Office of
2 Science and Technology Policy, acting through the
3 Networking and Information Technology Research
4 and Development Program, shall coordinate with the
5 Director of the National Science Foundation, the Di-
6 rector of the National Institute of Standards and
7 Technology, and the Commission to accelerate the
8 development and use of privacy enhancing tech-
9 nologies.

10 (2) OUTREACH.—The Director of the National
11 Institute of Standards and Technology shall conduct
12 outreach to—

13 (A) receive input from private, public, and
14 academic stakeholders on the development and
15 potential uses of privacy enhancing tech-
16 nologies; and

17 (B) develop ongoing public and private sec-
18 tor engagement to create and disseminate vol-
19 untary, consensus-based resources to increase
20 the integration of privacy enhancing tech-
21 nologies in data collection, sharing, transfers,
22 retention, and analytics by the public and pri-
23 vate sectors.

24 (d) REPORT ON RESEARCH AND STANDARDS DEVEL-
25 OPMENT.—Not later than 2 years after the date of enact-

1 ment of this Act, the Director of the Office of Science and
2 Technology Policy, acting through the Networking and In-
3 formation Technology Research and Development Pro-
4 gram, shall, in coordination with the Director of the Na-
5 tional Science Foundation, the Director of the National
6 Institute of Standards and Technology, and the Commis-
7 sion, submit to the Committee on Commerce, Science, and
8 Transportation of the Senate, the Subcommittee on Com-
9 merce, Justice, Science, and Related Agencies of the Com-
10 mittee on Appropriations of the Senate, the Committee on
11 Science, Space, and Technology of the House of Rep-
12 resentatives, and the Subcommittee on Commerce, Jus-
13 tice, Science, and Related Agencies of the Committee on
14 Appropriations of the House of Representatives, a report
15 containing—

16 (1) the progress of research on privacy enhanc-
17 ing technologies;

18 (2) the progress of the development of vol-
19 untary resources described under subsection
20 (c)(2)(B); and

21 (3) any policy recommendations of the Direc-
22 tors and the Commission that could facilitate and
23 improve communication and coordination between
24 the private sector, the National Science Foundation,

1 and relevant Federal agencies through the imple-
2 mentation of privacy enhancing technologies.

3 **SEC. 9. ENFORCEMENT.**

4 (a) ENFORCEMENT BY THE COMMISSION.—

5 (1) IN GENERAL.—This Act and the regulations
6 prescribed under this Act, other than the provisions
7 of and amendments made by section 8, shall be en-
8 forced by the Commission under the Federal Trade
9 Commission Act (15 U.S.C. 41 et seq.).

10 (2) UNFAIR OR DECEPTIVE ACTS OR PRAC-
11 TICES.—A violation of this Act or a regulation pre-
12 scribed under this Act shall be treated as a violation
13 of a rule defining an unfair or deceptive act or prac-
14 tice prescribed under section 18(a)(1)(B) of the Fed-
15 eral Trade Commission Act (15 U.S.C.
16 57a(a)(1)(B)).

17 (3) ACTIONS BY THE COMMISSION.—Subject to
18 paragraph (4), the Commission shall prevent any
19 person from violating this Act or a regulation pre-
20 scribed under this Act in the same manner, by the
21 same means, and with the same jurisdiction, powers,
22 and duties as though all applicable terms and provi-
23 sions of the Federal Trade Commission Act (15
24 U.S.C. 41 et seq.) were incorporated into and made
25 a part of this Act, and any person who violates this

1 Act or such regulation shall be subject to the pen-
2 alties and entitled to the privileges and immunities
3 provided in the Federal Trade Commission Act (15
4 U.S.C. 41 et seq.).

5 (4) COMMON CARRIERS.—Notwithstanding sec-
6 tion 4, 5(a)(2), or 6 of the Federal Trade Commis-
7 sion Act (15 U.S.C. 44, 45(a)(2), and 46) or any ju-
8 risdictional limitation of the Commission, the Com-
9 mission shall also enforce this Act, in the same man-
10 ner provided in paragraphs (1), (2), and (3) with re-
11 spect to common carriers subject to the Communica-
12 tions Act of 1934 (47 U.S.C. 151 et seq.) and Acts
13 amendatory thereof and supplementary thereto.

14 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-
15 ERAL.—

16 (1) IN GENERAL.—

17 (A) CIVIL ACTIONS.—In any case in which
18 the attorney general of a State has reason to
19 believe that an interest of the residents of that
20 State has been or is threatened or adversely af-
21 fected by the engagement of any person in a
22 practice that violates this Act or a regulation
23 prescribed under this Act, the State, as *parens*
24 *patriae*, may bring a civil action on behalf of
25 the residents of the State in a district court of

1 the United States of appropriate jurisdiction
2 to—

3 (i) enjoin that practice;

4 (ii) enforce compliance with this Act
5 or such regulation;

6 (iii) obtain damages, restitution, or
7 other compensation on behalf of residents
8 of the State;

9 (iv) impose a civil penalty in an
10 amount that is not greater than the prod-
11 uct of the number of individuals whose in-
12 formation was affected by a violation and
13 \$40,000; or

14 (v) obtain such other relief as the
15 court may consider to be appropriate.

16 (B) ADJUSTMENT FOR INFLATION.—Be-
17 ginning on the date that the Consumer Price
18 Index is first published by the Bureau of Labor
19 Statistics that is after 1 year after the date of
20 enactment of this Act, and each year thereafter,
21 the amounts specified in subparagraph (A)(iv)
22 shall be increased by the percentage increase in
23 the Consumer Price Index published on that
24 date from the Consumer Price Index published
25 the previous year.

1 (C) NOTICE.—

2 (i) IN GENERAL.—Before filing an ac-
3 tion under subparagraph (A), the attorney
4 general of the State involved shall provide
5 to the Commission—

6 (I) written notice of that action;

7 and

8 (II) a copy of the complaint for
9 that action.

10 (ii) EXEMPTION.—

11 (I) IN GENERAL.—Clause (i)
12 shall not apply with respect to the fil-
13 ing of an action by an attorney gen-
14 eral of a State under this paragraph
15 if the attorney general determines
16 that it is not feasible to provide the
17 notice described in that clause before
18 the filing of the action.

19 (II) NOTIFICATION.—In an ac-
20 tion described in subclause (I), the at-
21 torney general of a State shall provide
22 notice and a copy of the complaint to
23 the Commission at the same time as
24 the attorney general files the action.

25 (c) RIGHTS OF THE COMMISSION.—

1 (1) INTERVENTION BY THE COMMISSION.—The
2 Commission may intervene in any civil action
3 brought by the attorney general of a State under
4 subsection (b) and upon intervening—

5 (A) be heard on all matters arising in the
6 civil action; and

7 (B) file petitions for appeal of a decision in
8 the civil action.

9 (2) POWERS.—Nothing in this subsection may
10 be construed to prevent the attorney general of a
11 State from exercising the powers conferred on the
12 attorney general by the laws of the State to conduct
13 investigations, to administer oaths or affirmations,
14 or to compel the attendance of witnesses or the pro-
15 duction of documentary or other evidence.

16 (3) ACTION BY THE COMMISSION.—If the Com-
17 mission institutes a civil action for violation of this
18 title or a regulation promulgated under this title, no
19 attorney general of a State may bring a civil action
20 under subsection (b) against any defendant named
21 in the complaint of the Commission for violation of
22 this Act or a regulation promulgated under this Act
23 that is alleged in the complaint.

24 (d) VENUE AND SERVICE OF PROCESS.—

1 (1) VENUE.—Any action brought under sub-
2 section (b) may be brought in—

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

7 (B) another court of competent jurisdic-
8 tion.

9 (2) SERVICE OF PROCESS.—In an action
10 brought under subsection (b), process may be served
11 in any district in which the defendant—

12 (A) is an inhabitant; or

13 (B) may be found.

14 (e) ACTION OF OTHER STATE OFFICIALS.—

15 (1) IN GENERAL.—In addition to civil actions
16 brought by attorneys general under subsection (b),
17 any other officer of a State who is authorized by the
18 State to do so may bring a civil action under sub-
19 section (b), subject to the same requirements and
20 limitations that apply under this subsection to civil
21 actions brought by attorneys general.

22 (2) SAVINGS PROVISION.—Nothing in this sub-
23 section may be construed to prohibit an authorized
24 official of a State from initiating or continuing any

1 proceeding in a court of the State for a violation of
2 any civil or criminal law of the State.

3 (f) PRESERVATION OF AUTHORITY.—Nothing in this
4 Act shall be construed to limit the authority of the Federal
5 Trade Commission under any other provision of law.

6 **SEC. 10. ADDITIONAL ENFORCEMENT RESOURCES.**

7 (a) IN GENERAL.—Notwithstanding any other provi-
8 sion of law the Commission may, without regard to the
9 civil service laws (including regulations), appoint not more
10 than 300 additional personnel for the purposes of enforce-
11 ing privacy and data security laws and regulations.

12 (b) AUTHORIZATION OF APPROPRIATIONS.—There is
13 authorized to be appropriated to the Commission such
14 sums as may be necessary to carry out this section.

○