

117TH CONGRESS  
1ST SESSION

# S. 3065

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

---

IN THE SENATE OF THE UNITED STATES

OCTOBER 26, 2021

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”—

19 (A) means any software solution, technical  
20 processes, or other technological means of en-  
21 hancing the privacy and confidentiality of an in-  
22 dividual’s covered data in data or sets of data;  
23 and

24 (B) includes anonymization and pseudony-  
25 mization techniques, filtering tools, anti-track-

1           ing technology, differential privacy tools, syn-  
2           thetic data, and secure multi-party computa-  
3           tion.

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

8                   (A) direct or indirect financial loss;

9                   (B) stigmatization or reputational harm;

10                  (C) anxiety, embarrassment, fear, and  
11           other severe emotional trauma;

12                  (D) loss of economic opportunity; or

13                  (E) physical harm.

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

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

23           (10) PSEUDONYMOUS DATA.—The term “pseu-  
24           donymous data” means covered data that may only  
25           be linked to the identity of an individual or the iden-

1       tivity of a device associated with an individual if com-  
2       bined with separate information.

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

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

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

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

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

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

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

22               (14) THIRD PARTY SERVICE PROVIDER.—The  
23      term “third party service provider” means any cov-  
24      ered entity that collects, processes, stores, or dis-  
25      closes covered data at the direction of, and for the

1       sole benefit of, another covered entity under a con-  
2       tract.

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

9       **SEC. 3. REQUIRED PRIVACY NOTICE.**

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

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

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

23               (2) the purposes for and means by which the  
24       entity collects, processes, and stores the covered  
25       data;

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

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

8 **SEC. 4. REQUIRED DATA PRACTICES.**

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

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

21                         (A) REASONABLE.—

22                                 (i) IN GENERAL.—Except as provided  
23                                 in paragraph (3), covered data collection,  
24                                 processing, storage, and disclosure prac-

1 tices must meet a reasonable interest of  
2 the covered entity, including—

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

9 (II) relevant and appropriate  
10 product and service development and  
11 enhancement;

12 (III) preventing and detecting  
13 abuse, fraud, and other criminal activ-  
14 ity;

15 (IV) reasonable communications  
16 and marketing practices that follow  
17 best practices, rules, and ethical  
18 standards;

19 (V) engaging in scientific, med-  
20 ical, or statistical research that fol-  
21 lows commonly accepted ethical stand-  
22 ards; or

23 (VI) any other purpose for which  
24 the Commission considers to be rea-  
25 sonable.



1 (ii) CONSIDERATIONS.—In promul-  
2 gating regulations in accordance with this  
3 subparagraph, the Commission shall con-  
4 sider—

5 (I) the role of impact assess-  
6 ments in determining the privacy risk  
7 for high-risk processing;

8 (II) the sensitivity of the covered  
9 data; and

10 (III) the impact of such regula-  
11 tions on small business.

12 (B) EQUITABLE.—

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

18 (I) discriminatory targeted adver-  
19 tising practices;

20 (II) price, service, or employment  
21 opportunity discrimination; or

22 (III) any other practice the Com-  
23 mission considers likely to result in  
24 discrimination against a protected  
25 characteristic.

1 (ii) CONSIDERATIONS.—In promul-  
2 gating regulations in accordance with this  
3 subparagraph, the Commission shall con-  
4 sider—

5 (I) established civil rights laws,  
6 common law, and existing relevant  
7 consent decrees;

8 (II) the existing economic models  
9 and technology available in the digital  
10 advertising system;

11 (III) the role of algorithms and  
12 impact assessments; and

13 (IV) the impact of such regula-  
14 tions on small businesses.

15 (C) FORTHRIGHT.—

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

21 (I) the use of inconspicuous re-  
22 cording or tracking devices and meth-  
23 ods;

24 (II) the disclosure of covered  
25 data that a reasonable individual be-

1           believes to be the content of a private  
2           communication with another party or  
3           parties;

4                   (III) notices, interfaces, or other  
5           representations likely to mislead con-  
6           sumers; or

7                   (IV) any other practice that the  
8           Commission considers likely to mis-  
9           lead individuals regarding the pur-  
10          poses for and means by which covered  
11          data is collected, processed, stored, or  
12          disclosed.

13          (ii) CONSIDERATIONS.—In promul-  
14          gating regulations in accordance with this  
15          subparagraph, the Commission shall con-  
16          sider—

17                   (I) existing relevant consent de-  
18          crees;

19                   (II) the reasonable expectations  
20          of consumers;

21                   (III) research on deceptive prac-  
22          tices;

23                   (IV) the role of deceptive user  
24          interfaces; and

1 (V) the impact of such regula-  
2 tions on small businesses.

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

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

16 (A) before the covered entity collects or  
17 discloses sensitive data linked to the individual;  
18 or

19 (B) before the covered entity collects, proc-  
20 esses, stores, or discloses data for purposes  
21 which are outside the context of the relationship  
22 of the covered entity with the individual linked  
23 to the data, including—

24 (i) the use of covered data beyond  
25 what is necessary to provide, improve, or

1 market a good or service that the indi-  
2 vidual requests;

3 (ii) the processing or disclosure of  
4 covered data differs in material ways from  
5 the purposes described in the privacy pol-  
6 icy that was in effect when the data was  
7 collected; and

8 (iii) any other purpose that Commis-  
9 sion considers outside of context.

10 (4) DATA MINIMIZATION REQUIREMENTS.—Ex-  
11 cept as provided in subsection (b), require covered  
12 entities to—

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

18 (B) store covered data only as long as is  
19 reasonably necessary to carry out the purposes  
20 for which the data was collected.

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

24 (1) inhibit detection or prevention of a security  
25 risk or incident;

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

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

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

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

12           (1) upon the request of an individual, provide  
13 the individual with access to, or an accurate rep-  
14 resentation of, covered data linked to with the indi-  
15 vidual or the individual’s device stored by the cov-  
16 ered entity;

17           (2) upon the request of an individual, provide  
18 the individual with a means to dispute and resolve  
19 the accuracy or completeness of the covered data  
20 linked to the individual or the individual’s device  
21 stored by the entity;

22           (3) upon the request of an individual, delete  
23 any covered data that the covered entity stores  
24 linked to the individual or the individual’s device;  
25 and

1           (4) when technically feasible, upon the request  
2           of an individual, allow the individual to transmit or  
3           transfer covered data linked to the individual or the  
4           individual's device that is maintained by the entity  
5           to the individual in a format that is standardized  
6           and interoperable.

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

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

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

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

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

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

24          (e) CONSIDERATION.—The Commission shall allow a  
25          covered entity, by contract, to provide relevant obligations

1 to the individual under subsection (a) on behalf of a third  
2 party service provider that collects, processes, stores, or  
3 discloses covered data only on behalf of the covered entity.

4 **SEC. 6. INFORMATION SECURITY STANDARDS.**

5 (a) **REQUIRED DATA SECURITY PRACTICES.—**

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

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

16 (B) the sensitivity of the covered data col-  
17 lected, processed, and stored and the associated  
18 privacy risk;

19 (C) the currently available and widely ac-  
20 cepted technological, administrative, and phys-  
21 ical means to protect covered data under the  
22 control of the covered entity;

23 (D) the cost associated with implementing,  
24 maintaining, and regularly reviewing the safe-  
25 guards; and



1 (E) the impact of these requirements on  
2 small- and medium-sized businesses.

3 (2) LIMITATIONS.—In promulgating the regula-  
4 tions required under this section, the Commission  
5 shall consider a covered entity who is in compliance  
6 with existing information security laws that the  
7 Commission determines are sufficiently rigorous to  
8 be in compliance with this section with respect to  
9 particular types of covered data to the extent those  
10 types of covered data are covered by such law, in-  
11 cluding the following:

12 (A) Title V of the Gramm-Leach-Bliley Act  
13 (15 U.S.C. 6801 et seq.).

14 (B) The Health Information Technology  
15 for Economic and Clinical Health Act (42  
16 U.S.C. 17931).

17 (C) The Health Insurance Portability and  
18 Accountability Act of 1996 Security Rule (45  
19 CFR 160.103 and part 164).

20 (D) Any other existing law requiring a cov-  
21 ered entity to implement and maintain informa-  
22 tion security practices and procedures that the  
23 Commission determines to be sufficiently rig-  
24 orous.

1 **SEC. 7. PRIVACY PROTECTION OFFICERS.**

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

7 (1) educate employees about compliance re-  
8 quirements;

9 (2) train employees involved in data processing;

10 (3) conduct regular, comprehensive audits to  
11 ensure compliance and make records of the audits  
12 available to enforcement authorities upon request;

13 (4) maintain updated, clear, and understand-  
14 able records of all data security practices undertaken  
15 by the covered entity;

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

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

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

1 **SEC. 8. RESEARCH INTO PRIVACY ENHANCING TECH-**  
2 **NOLOGY.**

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

10 (1) fundamental research on technologies for  
11 de-identification, pseudonymization, anonymization,  
12 or obfuscation of covered data in data sets while  
13 maintaining fairness, accuracy, and efficiency;

14 (2) fundamental research on algorithms and  
15 other similar mathematical tools used to protect in-  
16 dividual privacy when collecting, storing, sharing, or  
17 aggregating data;

18 (3) fundamental research on technologies that  
19 promote data minimization principles in data collec-  
20 tion, sharing, and analytics; and

21 (4) research awards on privacy enhancing tech-  
22 nologies coordinated with other relevant Federal  
23 agencies and programs.

24 (b) INTEGRATION INTO THE COMPUTER AND NET-  
25 WORK SECURITY PROGRAM.—Subparagraph (D) of sec-  
26 tion 4(a)(1) of the Cyber Security Research and Develop-

1 ment Act (15 U.S.C. 7403(a)(1)(D)) is amended to read  
2 as follows:

3 “(D) privacy enhancing technologies and  
4 confidentiality;”.

5 (c) COORDINATION WITH THE NATIONAL INSTITUTE  
6 OF STANDARDS AND TECHNOLOGY AND OTHER STAKE-  
7 HOLDERS.—

8 (1) IN GENERAL.—The Director of the Office of  
9 Science and Technology Policy, acting through the  
10 Networking and Information Technology Research  
11 and Development Program, shall coordinate with the  
12 Director of the National Science Foundation, the Di-  
13 rector of the National Institute of Standards and  
14 Technology, and the Commission to accelerate the  
15 development and use of privacy enhancing tech-  
16 nologies.

17 (2) OUTREACH.—The Director of the National  
18 Institute of Standards and Technology shall conduct  
19 outreach to—

20 (A) receive input from private, public, and  
21 academic stakeholders, including the National  
22 Institutes of Health and the Centers for Dis-  
23 ease Control and Prevention, for the purpose of  
24 facilitating public health research, on the devel-  
25 opment of privacy enhancing technologies; and

1           (B) develop ongoing public and private sec-  
2           tor engagement to create and disseminate vol-  
3           untary, consensus-based resources to increase  
4           the integration of privacy enhancing tech-  
5           nologies in data collection, sharing, and ana-  
6           lytics by the public and private sectors.

7           (d) REPORT ON RESEARCH AND STANDARDS DEVEL-  
8           OPMENT.—Not later than 2 years after the date of enact-  
9           ment of this Act, the Director of the Office of Science and  
10          Technology Policy, acting through the Networking and In-  
11          formation Technology Research and Development Pro-  
12          gram, shall, in coordination with the Director of the Na-  
13          tional Science Foundation and the Director of the Na-  
14          tional Institute of Standards and Technology, submit to  
15          the Committee on Commerce, Science, and Transportation  
16          of the Senate, the Subcommittee on Commerce, Justice,  
17          Science, and Related Agencies of the Committee on Appro-  
18          priations of the Senate, the Committee on Science, Space,  
19          and Technology of the House of Representatives, and the  
20          Subcommittee on Commerce, Justice, Science, and Re-  
21          lated Agencies of the Committee on Appropriations of the  
22          House of Representatives, a report containing—

23                 (1) the progress of research on privacy enhance-  
24                 ing technologies;

1           (2) the progress of the development of vol-  
2           untary resources described under subsection  
3           (c)(2)(B); and

4           (3) any policy recommendations of the Direc-  
5           tors that could facilitate and improve communication  
6           and coordination between the private sector, the Na-  
7           tional Science Foundation, and relevant Federal  
8           agencies through the implementation of privacy en-  
9           hancing technologies.

10 **SEC. 9. ENFORCEMENT.**

11           (a) ENFORCEMENT BY THE COMMISSION.—

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

17           (2) UNFAIR OR DECEPTIVE ACTS OR PRAC-  
18           TICES.—A violation of this Act or a regulation pre-  
19           scribed under this Act shall be treated as a violation  
20           of a rule defining an unfair or deceptive act or prac-  
21           tice prescribed under section 18(a)(1)(B) of the Fed-  
22           eral Trade Commission Act (15 U.S.C.  
23           57a(a)(1)(B)).

24           (3) ACTIONS BY THE COMMISSION.—Subject to  
25           paragraph (4), the Commission shall prevent any

1 person from violating this Act or a regulation pre-  
2 scribed under this Act in the same manner, by the  
3 same means, and with the same jurisdiction, powers,  
4 and duties as though all applicable terms and provi-  
5 sions of the Federal Trade Commission Act (15  
6 U.S.C. 41 et seq.) were incorporated into and made  
7 a part of this Act, and any person who violates this  
8 Act or such regulation shall be subject to the pen-  
9 alties and entitled to the privileges and immunities  
10 provided in the Federal Trade Commission Act (15  
11 U.S.C. 41 et seq.).

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

21 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-  
22 ERAL.—

23 (1) IN GENERAL.—

24 (A) CIVIL ACTIONS.—In any case in which  
25 the attorney general of a State has reason to

1 believe that an interest of the residents of that  
2 State has been or is threatened or adversely af-  
3 fected by the engagement of any person in a  
4 practice that violates this Act or a regulation  
5 prescribed under this Act, the State, as *parens*  
6 *patriae*, may bring a civil action on behalf of  
7 the residents of the State in a district court of  
8 the United States of appropriate jurisdiction  
9 to—

10 (i) enjoin that practice;

11 (ii) enforce compliance with this Act  
12 or such regulation;

13 (iii) obtain damages, restitution, or  
14 other compensation on behalf of residents  
15 of the State;

16 (iv) impose a civil penalty in an  
17 amount that is not greater than the prod-  
18 uct of the number of individuals whose in-  
19 formation was affected by a violation and  
20 \$40,000; or

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

23 (B) ADJUSTMENT FOR INFLATION.—Be-  
24 ginning on the date that the Consumer Price  
25 Index is first published by the Bureau of Labor



1 Statistics that is after 1 year after the date of  
2 enactment of this Act, and each year thereafter,  
3 the amounts specified in subparagraph (A)(iv)  
4 shall be increased by the percentage increase in  
5 the Consumer Price Index published on that  
6 date from the Consumer Price Index published  
7 the previous year.

8 (C) NOTICE.—

9 (i) IN GENERAL.—Before filing an ac-  
10 tion under subparagraph (A), the attorney  
11 general of the State involved shall provide  
12 to the Commission—

13 (I) written notice of that action;

14 and

15 (II) a copy of the complaint for  
16 that action.

17 (ii) EXEMPTION.—

18 (I) IN GENERAL.—Clause (i)  
19 shall not apply with respect to the fil-  
20 ing of an action by an attorney gen-  
21 eral of a State under this paragraph  
22 if the attorney general determines  
23 that it is not feasible to provide the  
24 notice described in that clause before  
25 the filing of the action.

1 (II) NOTIFICATION.—In an ac-  
2 tion described in subclause (I), the at-  
3 torney general of a State shall provide  
4 notice and a copy of the complaint to  
5 the Commission at the same time as  
6 the attorney general files the action.

7 (c) RIGHTS OF THE COMMISSION.—

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

12 (A) be heard on all matters arising in the  
13 civil action; and

14 (B) file petitions for appeal of a decision in  
15 the civil action.

16 (2) POWERS.—Nothing in this subsection may  
17 be construed to prevent the attorney general of a  
18 State from exercising the powers conferred on the  
19 attorney general by the laws of the State to conduct  
20 investigations, to administer oaths or affirmations,  
21 or to compel the attendance of witnesses or the pro-  
22 duction of documentary or other evidence.

23 (3) ACTION BY THE COMMISSION.—If the Com-  
24 mission institutes a civil action for violation of this  
25 title or a regulation promulgated under this title, no

1 attorney general of a State may bring a civil action  
2 under subsection (b) against any defendant named  
3 in the complaint of the Commission for violation of  
4 this Act or a regulation promulgated under this Act  
5 that is alleged in the complaint.

6 (d) VENUE AND SERVICE OF PROCESS.—

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

9 (A) the district court of the United States  
10 that meets applicable requirements relating to  
11 venue under section 1391 of title 28, United  
12 States Code; or

13 (B) another court of competent jurisdic-  
14 tion.

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

18 (A) is an inhabitant; or

19 (B) may be found.

20 (e) ACTION OF OTHER STATE OFFICIALS.—

21 (1) IN GENERAL.—In addition to civil actions  
22 brought by attorneys general under subsection (b),  
23 any other officer of a State who is authorized by the  
24 State to do so may bring a civil action under sub-  
25 section (b), subject to the same requirements and

1 limitations that apply under this subsection to civil  
2 actions brought by attorneys general.

3 (2) SAVINGS PROVISION.—Nothing in this sub-  
4 section may be construed to prohibit an authorized  
5 official of a State from initiating or continuing any  
6 proceeding in a court of the State for a violation of  
7 any civil or criminal law of the State.

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

11 **SEC. 10. ADDITIONAL ENFORCEMENT RESOURCES.**

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

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

○