

115TH CONGRESS  
1ST SESSION

# S. 2187

To establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission, to amend the Children's Online Privacy Protection Act of 1998 to improve provisions relating to collection, use, and disclosure of personal information of children, and for other purposes.

---

IN THE SENATE OF THE UNITED STATES

DECEMBER 4, 2017

Mr. MENENDEZ introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

## A BILL

To establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission, to amend the Children's Online Privacy Protection Act of 1998 to improve provisions relating to collection, use, and disclosure of personal information of children, 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. TABLE OF CONTENTS.**

4 The table of contents for this Act is as follows:

Sec. 1. Table of contents.

## TITLE I—COMMERCIAL PRIVACY

- Sec. 101. Short title.
- Sec. 102. Findings.
- Sec. 103. Definitions.

## Subtitle A—Right to Security and Accountability

- Sec. 111. Security.
- Sec. 112. Accountability.
- Sec. 113. Privacy by design.

## Subtitle B—Right to Notice and Individual Participation

- Sec. 121. Transparent notice of practices and purposes.
- Sec. 122. Individual participation.

## Subtitle C—Rights Relating to Data Minimization, Constraints on Distribution, and Data Integrity

- Sec. 131. Data minimization.
- Sec. 132. Constraints on distribution of information.
- Sec. 133. Data integrity.

## Subtitle D—Right to Notice of Breaches of Security

- Sec. 141. Definitions.
- Sec. 142. Notice to individuals.
- Sec. 143. Notice to law enforcement.

## Subtitle E—Enforcement

- Sec. 151. General application.
- Sec. 152. Enforcement by the Federal Trade Commission.
- Sec. 153. Enforcement by Attorney General.
- Sec. 154. Enforcement by States.
- Sec. 155. Civil penalties.
- Sec. 156. Effect on other laws.
- Sec. 157. No private right of action.

## Subtitle F—Co-Regulatory Safe Harbor Programs

- Sec. 161. Establishment of safe harbor programs.
- Sec. 162. Participation in safe harbor program.

## Subtitle G—Application With Other Federal Laws

- Sec. 171. Application with other Federal laws.

## Subtitle H—Development of Commercial Data Privacy Policy in the Department of Commerce

- Sec. 181. Direction to develop commercial data privacy policy.

## TITLE II—ONLINE PRIVACY OF CHILDREN

- Sec. 201. Short title.
- Sec. 202. Findings.
- Sec. 203. Definitions.

Sec. 204. Online collection, use, and disclosure of personal information of children.

Sec. 205. Targeted marketing to children or minors.

Sec. 206. Digital Marketing Bill of Rights for Teens and Fair Information Practices Principles.

Sec. 207. Online collection of geolocation information of children and minors.

Sec. 208. Removal of content.

Sec. 209. Enforcement and applicability.

Sec. 210. Rule for treatment of users of websites, services, and applications directed to children or minors.

Sec. 211. Effective dates.

## 1 **TITLE I—COMMERCIAL PRIVACY**

### 2 **SEC. 101. SHORT TITLE.**

3       This title may be cited as the “Commercial Privacy  
4 Bill of Rights Act of 2017”.

### 5 **SEC. 102. FINDINGS.**

6       The Congress finds the following:

7           (1) Personal privacy is worthy of protection  
8 through appropriate legislation.

9           (2) Trust in the treatment of personally identi-  
10 fiable information collected on and off the Internet  
11 is essential for businesses to succeed.

12           (3) Persons interacting with others engaged in  
13 interstate commerce have a significant interest in  
14 their personal information, as well as a right to con-  
15 trol how that information is collected, used, stored,  
16 or transferred.

17           (4) Persons engaged in interstate commerce  
18 and collecting personally identifiable information on  
19 individuals have a responsibility to treat that infor-

1       mation with respect and in accordance with common  
2       standards.

3           (5) On the day before the date of enactment of  
4       this Act, the laws of the Federal Government and  
5       State and local governments provided inadequate  
6       privacy protection for individuals engaging in and  
7       interacting with persons engaged in interstate com-  
8       merce.

9           (6) As of the day before the date of enactment  
10       of this Act, with the exception of Federal Trade  
11       Commission enforcement of laws against unfair and  
12       deceptive practices, the Federal Government has es-  
13       chewed general commercial privacy laws in favor of  
14       industry self-regulation, which has led to several  
15       self-policing schemes, some of which are enforceable,  
16       and some of which provide insufficient privacy pro-  
17       tection to individuals.

18          (7) As of the day before the date of enactment  
19       of this Act, many collectors of personally identifiable  
20       information have yet to provide baseline fair infor-  
21       mation practice protections for individuals.

22          (8) The ease of gathering and compiling per-  
23       sonal information on the Internet and off, both  
24       overtly and surreptitiously, is becoming increasingly  
25       efficient and effortless due to advances in technology

1       which have provided information gatherers the abil-  
2       ity to compile seamlessly highly detailed personal  
3       histories of individuals.

4           (9) Personal information requires greater pri-  
5       vacy protection than is available on the day before  
6       the date of enactment of this Act. Vast amounts of  
7       personal information, including sensitive informa-  
8       tion, about individuals are collected on and off the  
9       Internet, often combined and sold or otherwise  
10      transferred to third parties, for purposes unknown  
11      to an individual to whom the personally identifiable  
12      information pertains.

13          (10) Toward the close of the 20th century, as  
14      individuals' personal information was increasingly  
15      collected, profiled, and shared for commercial pur-  
16      poses, and as technology advanced to facilitate these  
17      practices, Congress enacted numerous statutes to  
18      protect privacy.

19          (11) Those statutes apply to the Government,  
20      telephones, cable television, e-mail, video tape rent-  
21      als, and the Internet (but only with respect to chil-  
22      dren and law enforcement requests).

23          (12) As in those instances, the Federal Govern-  
24      ment has a substantial interest in creating a level  
25      playing field of protection across all collectors of per-

1       sonally identifiable information, both in the United  
2       States and abroad.

3           (13) Enhancing individual privacy protection in  
4       a balanced way that establishes clear, consistent  
5       rules, both domestically and internationally, will  
6       stimulate commerce by instilling greater consumer  
7       confidence at home and greater confidence abroad as  
8       more and more entities digitize personally identifi-  
9       able information, whether collected, stored, or used  
10      online or offline.

11   **SEC. 103. DEFINITIONS.**

12       (a) IN GENERAL.—Subject to subsection (b), in this  
13      title:

14           (1) COMMISSION.—The term “Commission”  
15      means the Federal Trade Commission.

16           (2) COVERED ENTITY.—The term “covered en-  
17      tity” means any person to whom this title applies  
18      under section 151.

19           (3) COVERED INFORMATION.—

20               (A) IN GENERAL.—Except as provided in  
21              subparagraph (B), the term “covered informa-  
22              tion” means only the following:

- 23                   (i) Personally identifiable information.
- 24                   (ii) Unique identifier information.

1 (iii) Any information that is collected,  
2 used, or stored in connection with person-  
3 ally identifiable information or unique  
4 identifier information in a manner that  
5 may reasonably be used by the party col-  
6 lecting the information to identify a spe-  
7 cific individual.

8 (B) EXCEPTION.—The term “covered in-  
9 formation” does not include the following:

10 (i) Personally identifiable information  
11 obtained from public records that is not  
12 merged with covered information gathered  
13 elsewhere.

14 (ii) Personally identifiable information  
15 that is obtained from a forum—

16 (I) where the individual volun-  
17 tarily shared the information or au-  
18 thorized the information to be shared;  
19 and

20 (II) that—

21 (aa) is widely and publicly  
22 available and was not made pub-  
23 licly available in bad faith; and

1 (bb) contains no restrictions  
 2 on who can access and view such  
 3 information.

4 (iii) Personally identifiable informa-  
 5 tion reported in public media.

6 (iv) Personally identifiable informa-  
 7 tion dedicated to contacting an individual  
 8 at the individual's place of work.

9 (4) ESTABLISHED BUSINESS RELATIONSHIP.—

10 The term “established business relationship” means,  
 11 with respect to a covered entity and a person, a rela-  
 12 tionship formed with or without the exchange of con-  
 13 sideration, involving the establishment of an account  
 14 by the person with the covered entity for the receipt  
 15 of products or services offered by the covered entity.

16 (5) PERSONALLY IDENTIFIABLE INFORMA-  
 17 TION.—The term “personally identifiable informa-  
 18 tion” means only the following:

19 (A) Any of the following information about  
 20 an individual:

21 (i) The first name (or initial) and last  
 22 name of an individual, whether given at  
 23 birth or time of adoption, or resulting from  
 24 a lawful change of name.

1 (ii) The postal address of a physical  
2 place of residence of such individual.

3 (iii) An e-mail address.

4 (iv) A telephone number or mobile de-  
5 vice number.

6 (v) A Social Security number or other  
7 Government issued identification number  
8 issued to such individual.

9 (vi) The account number of a credit  
10 card issued to such individual.

11 (vii) Unique identifier information  
12 that alone can be used to identify a spe-  
13 cific individual.

14 (viii) Biometric data about such indi-  
15 vidual, including fingerprints and retina  
16 scans.

17 (B) If used, transferred, or stored in con-  
18 nection with one or more of the items of infor-  
19 mation described in subparagraph (A), any of  
20 the following:

21 (i) A date of birth.

22 (ii) The number of a certificate of  
23 birth or adoption.

24 (iii) A place of birth.

1 (iv) Unique identifier information that  
 2 alone cannot be used to identify a specific  
 3 individual.

4 (v) Precise geographic location, at the  
 5 same degree of specificity as a global posi-  
 6 tioning system or equivalent system, and  
 7 not including any general geographic infor-  
 8 mation that may be derived from an Inter-  
 9 net Protocol address.

10 (vi) Information about an individual's  
 11 quantity, technical configuration, type, des-  
 12 tination, location, and amount of uses of  
 13 voice services, regardless of technology  
 14 used.

15 (vii) Any other information concerning  
 16 an individual that may reasonably be used  
 17 by the party using, collecting, or storing  
 18 that information to identify that individual.

19 (6) SENSITIVE PERSONALLY IDENTIFIABLE IN-  
 20 FORMATION.—The term “sensitive personally identi-  
 21 fiable information” means—

22 (A) personally identifiable information  
 23 which, if lost, compromised, or disclosed with-  
 24 out authorization either alone or with other in-

1 formation, carries a significant risk of economic  
2 or physical harm; or

3 (B) information related to—

4 (i) a particular medical condition or a  
5 health record; or

6 (ii) the religious affiliation of an indi-  
7 vidual.

8 (7) THIRD PARTY.—

9 (A) IN GENERAL.—The term “third party”  
10 means, with respect to a covered entity, a per-  
11 son that—

12 (i) is—

13 (I) not related to the covered en-  
14 tity by common ownership or cor-  
15 porate control; or

16 (II) related to the covered entity  
17 by common ownership or corporate  
18 control and an ordinary consumer  
19 would not understand that the covered  
20 entity and the person were related by  
21 common ownership or corporate con-  
22 trol;

23 (ii) is not a service provider used by  
24 the covered entity to receive personally  
25 identifiable information or sensitive person-

1           ally identifiable information in performing  
 2           services or functions on behalf of and  
 3           under the instruction of the covered entity;  
 4           and

5           (iii) with respect to the collection of  
 6           covered information of an individual, does  
 7           not have an established business relation-  
 8           ship with the individual and does not iden-  
 9           tify itself to the individual at the time of  
 10          such collection in a clear and conspicuous  
 11          manner that is visible to the individual.

12          (B) COMMON BRANDS.—The term “third  
 13          party” may include, with respect to a covered  
 14          entity, a person who operates under a common  
 15          brand with the covered entity.

16          (8) UNAUTHORIZED USE.—

17          (A) IN GENERAL.—The term “unauthor-  
 18          ized use” means the use of covered information  
 19          by a covered entity or its service provider for  
 20          any purpose not authorized by the individual to  
 21          whom such information relates.

22          (B) EXCEPTIONS.—Except as provided in  
 23          subparagraph (C), the term “unauthorized use”  
 24          does not include use of covered information re-

1           lating to an individual by a covered entity or its  
2           service provider as follows:

3                   (i) To process and enforce a trans-  
4                   action or deliver a service requested by  
5                   that individual.

6                   (ii) To operate the covered entity that  
7                   is providing a transaction or delivering a  
8                   service requested by that individual, such  
9                   as inventory management, financial report-  
10                  ing and accounting, planning, and product  
11                  or service improvement or forecasting.

12                  (iii) To prevent or detect fraud or to  
13                  provide for a physically or virtually secure  
14                  environment.

15                  (iv) To investigate a possible crime.

16                  (v) That is required by a provision of  
17                  law or legal process.

18                  (vi) To market or advertise to an indi-  
19                  vidual from a covered entity within the  
20                  context of a covered entity's own Internet  
21                  website, services, or products if the covered  
22                  information used for such marketing or ad-  
23                  vertising was—

24                           (I) collected directly by the cov-  
25                           ered entity; or

1 (II) shared with the covered enti-  
2 ty—

3 (aa) at the affirmative re-  
4 quest of the individual; or

5 (bb) by an entity with which  
6 the individual has an established  
7 business relationship.

8 (vii) Use that is necessary for the im-  
9 provement of transaction or service deliv-  
10 ery through research, testing, analysis, and  
11 development.

12 (viii) Use that is necessary for inter-  
13 nal operations, including the following:

14 (I) Collecting customer satisfac-  
15 tion surveys and conducting customer  
16 research to improve customer service  
17 information.

18 (II) Information collected by an  
19 Internet website about the visits to  
20 such website and the click-through  
21 rates at such website—

22 (aa) to improve website  
23 navigation and performance; or

24 (bb) to understand and im-  
25 prove the interaction of an indi-

1                   vidual with the advertising of a  
2                   covered entity.

3                   (ix) Use—

4                   (I) by a covered entity with  
5                   which an individual has an established  
6                   business relationship;

7                   (II) which the individual could  
8                   have reasonably expected, at the time  
9                   such relationship was established, was  
10                  related to a service provided pursuant  
11                  to such relationship; and

12                  (III) which does not constitute a  
13                  material change in use or practice  
14                  from what could have reasonably been  
15                  expected.

16                  (C) SAVINGS.—A use of covered informa-  
17                  tion regarding an individual by a covered entity  
18                  or its service provider may only be excluded  
19                  under subparagraph (B) from the definition of  
20                  “unauthorized use” under subparagraph (A) if  
21                  the use is reasonable and consistent with the  
22                  practices and purposes described in the notice  
23                  given the individual in accordance with section  
24                  121(a)(1).

1           (9) UNIQUE IDENTIFIER INFORMATION.—The  
 2       term “unique identifier information” means a  
 3       unique persistent identifier associated with an indi-  
 4       vidual or a networked device, including a customer  
 5       number held in a cookie, a user identification, a  
 6       processor serial number, or a device serial number.

7       (b) MODIFIED DEFINITION BY RULEMAKING.—If the  
 8       Commission determines that a term defined in any of  
 9       paragraphs (3) through (8) is not reasonably sufficient to  
 10      protect an individual from unfair or deceptive acts or prac-  
 11      tices, the Commission may by rule modify such definition  
 12      as the Commission considers appropriate to protect such  
 13      individual from an unfair or deceptive act or practice to  
 14      the extent that the Commission determines will not unrea-  
 15      sonably impede interstate commerce.

## 16       **Subtitle A—Right to Security and** 17               **Accountability**

### 18       **SEC. 111. SECURITY.**

19       (a) RULEMAKING REQUIRED.—Not later than 180  
 20      days after the date of enactment of this Act, the Commis-  
 21      sion shall initiate a rulemaking proceeding to require each  
 22      covered entity to carry out security measures to protect  
 23      the covered information it collects and maintains.

24       (b) PROPORTION.—The requirements prescribed  
 25      under subsection (a) shall provide for security measures

1 that are proportional to the size, type, nature, and sensi-  
 2 tivity of the covered information a covered entity collects.

3 (c) CONSISTENCY.—The requirements prescribed  
 4 under subsection (a) shall be consistent with guidance pro-  
 5 vided by the Commission and recognized industry prac-  
 6 tices for safety and security on the day before the date  
 7 of enactment of this Act.

8 (d) TECHNOLOGICAL MEANS.—In a rule prescribed  
 9 under subsection (a), the Commission may not require a  
 10 specific technological means of meeting a requirement.

11 **SEC. 112. ACCOUNTABILITY.**

12 Each covered entity shall, in a manner proportional  
 13 to the size, type, and nature of the covered information  
 14 it collects—

15 (1) have managerial accountability, proportional  
 16 to the size and structure of the covered entity, for  
 17 the adoption and implementation of policies con-  
 18 sistent with this title;

19 (2) have a process to respond to non-frivolous  
 20 inquiries from individuals regarding the collection,  
 21 use, transfer, or storage of covered information re-  
 22 lating to such individuals; and

23 (3) describe the means of compliance of the cov-  
 24 ered entity with the requirements of this Act upon  
 25 request from—

1 (A) the Commission; or

2 (B) an appropriate safe harbor program  
3 established under section 151.

4 **SEC. 113. PRIVACY BY DESIGN.**

5 Each covered entity shall, in a manner proportional  
6 to the size, type, and nature of the covered information  
7 that it collects, implement a comprehensive information  
8 privacy program by—

9 (1) incorporating necessary development proc-  
10 esses and practices throughout the product life cycle  
11 that are designed to safeguard the personally identi-  
12 fiable information that is covered information of in-  
13 dividuals based on—

14 (A) the reasonable expectations of such in-  
15 dividuals regarding privacy; and

16 (B) the relevant threats that need to be  
17 guarded against in meeting those expectations;  
18 and

19 (2) maintaining appropriate management proc-  
20 esses and practices throughout the data life cycle  
21 that are designed to ensure that information systems  
22 comply with—

23 (A) the provisions of this title;

24 (B) the privacy policies of a covered entity;

25 and

1 (C) the privacy preferences of individuals  
 2 that are consistent with the consent choices and  
 3 related mechanisms of individual participation  
 4 as described in section 122.

## 5 **Subtitle B—Right to Notice and** 6 **Individual Participation**

### 7 **SEC. 121. TRANSPARENT NOTICE OF PRACTICES AND PUR-** 8 **POSES.**

9 (a) IN GENERAL.—Not later than 60 days after the  
 10 date of enactment of this Act, the Commission shall ini-  
 11 tiate a rulemaking proceeding to require each covered enti-  
 12 ty—

13 (1) to provide accurate, clear, concise, and  
 14 timely notice to individuals of—

15 (A) the practices of the covered entity re-  
 16 garding the collection, use, transfer, and stor-  
 17 age of covered information; and

18 (B) the specific purposes of those prac-  
 19 tices;

20 (2) to provide accurate, clear, concise, and  
 21 timely notice to individuals before implementing a  
 22 material change in such practices; and

23 (3) to maintain the notice required by para-  
 24 graph (1) in a form that individuals can readily ac-  
 25 cess.

1 (b) COMPLIANCE AND OTHER CONSIDERATIONS.—In  
 2 the rulemaking required by subsection (a), the Commis-  
 3 sion—

4 (1) shall consider the types of devices and  
 5 methods individuals will use to access the required  
 6 notice;

7 (2) may provide that a covered entity unable to  
 8 provide the required notice when information is col-  
 9 lected may comply with the requirement of sub-  
 10 section (a)(1) by providing an alternative time and  
 11 means for an individual to receive the required no-  
 12 tice promptly;

13 (3) may draft guidance for covered entities to  
 14 use in designing their own notice and may include  
 15 a draft model template for covered entities to use in  
 16 designing their own notice; and

17 (4) may provide guidance on how to construct  
 18 computer-readable notices or how to use other tech-  
 19 nology to deliver the required notice.

20 **SEC. 122. INDIVIDUAL PARTICIPATION.**

21 (a) IN GENERAL.—Not later than 180 days after the  
 22 date of enactment of this Act, the Commission shall ini-  
 23 tiate a rulemaking proceeding to require each covered enti-  
 24 ty—

1           (1) to offer individuals a clear and conspicuous  
2           mechanism for opt-in consent for any use of their  
3           covered information that would otherwise be unau-  
4           thorized use;

5           (2) to offer individuals a robust, clear, and con-  
6           spicuous mechanism for opt-in consent for the use  
7           by third parties of the individuals' covered informa-  
8           tion for behavioral advertising or marketing;

9           (3) to provide any individual to whom the per-  
10          sonally identifiable information that is covered infor-  
11          mation pertains, and which the covered entity or its  
12          service provider stores, appropriate and reasonable—

13                 (A) access to such information; and

14                 (B) mechanisms to correct such informa-  
15          tion to improve the accuracy of such informa-  
16          tion; and

17          (4) in the case that a covered entity enters  
18          bankruptcy or an individual requests the termination  
19          of a service provided by the covered entity to the in-  
20          dividual or termination of some other relationship  
21          with the covered entity, to permit the individual to  
22          easily request that—

23                 (A) all of the personally identifiable infor-  
24          mation that is covered information that the cov-  
25          ered entity maintains relating to the individual,

1           except for information the individual authorized  
2           the sharing of or which the individual shared  
3           with the covered entity in a forum that is wide-  
4           ly and publicly available, be rendered not per-  
5           sonally identifiable; or

6                   (B) if rendering such information not per-  
7           sonally identifiable is not possible, to cease the  
8           unauthorized use or transfer to a third party  
9           for an unauthorized use of such information or  
10          to cease use of such information for marketing,  
11          unless such unauthorized use or transfer is oth-  
12          erwise required by a provision of law.

13          (b) UNAUTHORIZED USE TRANSFERS.—In the rule-  
14   making required by subsection (a), the Commission shall  
15   provide that with respect to transfers of covered informa-  
16   tion to a third party for which an individual provides opt-  
17   in consent, the third party to which the information is  
18   transferred may not use such information for any unau-  
19   thorized use other than a use—

20                   (1) specified pursuant to the purposes stated in  
21   the required notice under section 121(a); and

22                   (2) authorized by the individual when the indi-  
23   vidual granted consent for the transfer of the infor-  
24   mation to the third party.

1       (c) ALTERNATIVE MEANS TO TERMINATE USE OF  
 2 COVERED INFORMATION.—In the rulemaking required by  
 3 subsection (a), the Commission shall allow a covered entity  
 4 to provide individuals an alternative means, in lieu of the  
 5 access, consent, and correction requirements, of prohib-  
 6 iting a covered entity from use or transfer of that individ-  
 7 ual’s covered information.

8       (d) SERVICE PROVIDERS.—

9           (1) IN GENERAL.—The use of a service provider  
 10 by a covered entity to receive covered information in  
 11 performing services or functions on behalf of and  
 12 under the instruction of the covered entity does not  
 13 constitute an unauthorized use of such information  
 14 by the covered entity if the covered entity and the  
 15 service provider execute a contract that requires the  
 16 service provider to collect, use, and store the infor-  
 17 mation on behalf of the covered entity in a manner  
 18 consistent with—

19                   (A) the requirements of this title; and

20                   (B) the policies and practices related to  
 21 such information of the covered entity.

22       (2) TRANSFERS BETWEEN SERVICE PROVIDERS  
 23 FOR A COVERED ENTITY.—The disclosure by a serv-  
 24 ice provider of covered information pursuant to a  
 25 contract with a covered entity to another service pro-

1 vider in order to perform the same service or func-  
 2 tions for that covered entity does not constitute an  
 3 unauthorized use.

4 (3) LIABILITY REMAINS WITH COVERED ENTI-  
 5 TY.—A covered entity remains responsible and liable  
 6 for the protection of covered information that has  
 7 been transferred to a service provider for processing,  
 8 notwithstanding any agreement to the contrary be-  
 9 tween a covered entity and the service provider.

## 10 **Subtitle C—Rights Relating to Data** 11 **Minimization, Constraints on** 12 **Distribution, and Data Integrity**

### 13 **SEC. 131. DATA MINIMIZATION.**

14 Each covered entity shall—

15 (1) collect only as much covered information re-  
 16 lating to an individual as is reasonably necessary—

17 (A) to process or enforce a transaction or  
 18 deliver a service requested by such individual;

19 (B) for the covered entity to provide a  
 20 transaction or delivering a service requested by  
 21 such individual, such as inventory management,  
 22 financial reporting and accounting, planning,  
 23 product or service improvement or forecasting,  
 24 and customer support and service;

1 (C) to prevent or detect fraud or to provide  
2 for a secure environment;

3 (D) to investigate a possible crime;

4 (E) to comply with a provision of law;

5 (F) for the covered entity to market or ad-  
6 vertise to such individual if the covered infor-  
7 mation used for such marketing or advertising  
8 was collected directly by the covered entity; or

9 (G) for internal operations, including—

10 (i) collecting customer satisfaction  
11 surveys and conducting customer research  
12 to improve customer service; and

13 (ii) collection from an Internet website  
14 of information about visits and click-  
15 through rates relating to such website to  
16 improve—

17 (I) website navigation and per-  
18 formance; and

19 (II) the customer's experience;

20 (2) retain covered information for only such du-  
21 ration as—

22 (A) with respect to the provision of a  
23 transaction or delivery of a service to an indi-  
24 vidual—

1 (i) is necessary to provide such trans-  
 2 action or deliver such service to such indi-  
 3 vidual; or

4 (ii) if such service is ongoing, is rea-  
 5 sonable for the ongoing nature of the serv-  
 6 ice; or

7 (B) is required by a provision of law;

8 (3) retain covered information only for the pur-  
 9 pose it was collected, or reasonably related purposes;  
 10 and

11 (4) exercise reasonable data retention proce-  
 12 dures with respect to both the initial collection and  
 13 subsequent retention.

14 **SEC. 132. CONSTRAINTS ON DISTRIBUTION OF INFORMA-**  
 15 **TION.**

16 (a) IN GENERAL.—Each covered entity shall—

17 (1) require by contract that any third party to  
 18 which it transfers covered information use the infor-  
 19 mation only for purposes that are consistent with—

20 (A) the provisions of this title; and

21 (B) as specified in the contract;

22 (2) require by contract that such third party  
 23 may not combine information that the covered entity  
 24 has transferred to it, that relates to an individual,  
 25 and that is not personally identifiable information

1 with other information in order to identify such indi-  
 2 vidual, unless the covered entity has obtained the  
 3 opt-in consent of such individual for such combina-  
 4 tion and identification; and

5 (3) before executing a contract with a third  
 6 party—

7 (A) assure through due diligence that the  
 8 third party is a legitimate organization; and

9 (B) in the case of a material violation of  
 10 the contract, at a minimum notify the Commis-  
 11 sion of such violation.

12 (b) TRANSFERS TO UNRELIABLE THIRD PARTIES  
 13 PROHIBITED.—A covered entity may not transfer covered  
 14 information to a third party that the covered entity  
 15 knows—

16 (1) has intentionally or willfully violated a con-  
 17 tract required by subsection (a); and

18 (2) is reasonably likely to violate such contract.

19 (c) APPLICATION OF RULES TO THIRD PARTIES.—

20 (1) IN GENERAL.—Except as provided in para-  
 21 graph (2), a third party that receives covered infor-  
 22 mation from a covered entity shall be subject to the  
 23 provisions of this Act as if it were a covered entity.

24 (2) EXEMPTION.—The Commission may, as it  
 25 determines appropriate, exempt classes of third par-

1       ties from liability under any provision of subtitle B  
2       if the Commission finds that—

3               (A) such class of third parties cannot rea-  
4               sonably comply with such provision; or

5               (B) with respect to covered information re-  
6               lating to individuals that is transferred to such  
7               class, compliance by such class with such provi-  
8               sion would not sufficiently benefit such individ-  
9               uals.

10 **SEC. 133. DATA INTEGRITY.**

11       (a) IN GENERAL.—Each covered entity shall attempt  
12       to establish and maintain reasonable procedures to ensure  
13       that personally identifiable information that is covered in-  
14       formation and maintained by the covered entity is accu-  
15       rate in those instances where the covered information  
16       could be used to deny consumers benefits or cause signifi-  
17       cant harm.

18       (b) EXCEPTION.—Subsection (a) shall not apply to  
19       covered information of an individual maintained by a cov-  
20       ered entity that is provided—

21               (1) directly to the covered entity by the indi-  
22       vidual;

23               (2) to the covered entity by another entity at  
24       the request of the individual;

25               (3) to prevent or detect fraud; or

(4) to provide for a secure environment.

## **Subtitle D—Right to Notice of Breaches of Security**

### **SEC. 141. DEFINITIONS.**

In this subtitle:

#### **(1) BREACH OF SECURITY.—**

(A) **IN GENERAL.**—The term “breach of security” means compromise of the security, confidentiality, or integrity of, or loss of, data in electronic form that results in, or there is a reasonable basis to conclude has resulted in, unauthorized access to or acquisition of personally identifiable information from a covered entity.

(B) **EXCLUSIONS.**—The term “breach of security” does not include—

(i) a good faith acquisition of personally identifiable information by a covered entity, or an employee or agent of a covered entity, if the personally identifiable information is not subject to further use or unauthorized disclosure;

(ii) any lawfully authorized investigative, protective, or intelligence activity of a law enforcement or an intelligence agency

1 of the United States, a State, or a political  
2 subdivision of a State; or

3 (iii) the release of a public record not  
4 otherwise subject to confidentiality or non-  
5 disclosure requirements.

6 (2) DATA IN ELECTRONIC FORM.—The term  
7 “data in electronic form” means any data stored  
8 electronically or digitally on any computer system or  
9 other database, including recordable tapes and other  
10 mass storage devices.

11 (3) DESIGNATED ENTITY.—The term “des-  
12 ignated entity” means the Federal Government enti-  
13 ty designated by the Secretary of Homeland Security  
14 under section 143(a).

15 (4) IDENTITY THEFT.—The term “identity  
16 theft” means the unauthorized use of another per-  
17 son’s personally identifiable information for the pur-  
18 pose of engaging in commercial transactions under  
19 the identity of such other person, including any con-  
20 tact that violates section 1028A of title 18, United  
21 States Code.

22 (5) MAJOR CREDIT REPORTING AGENCY.—The  
23 term “major credit reporting agency” means a con-  
24 sumer reporting agency that compiles and maintains  
25 files on consumers on a nationwide basis within the

1 meaning of section 603(p) of the Fair Credit Re-  
2 porting Act (15 U.S.C. 1681a(p)).

3 (6) SERVICE PROVIDER.—The term “service  
4 provider” means a person that provides electronic  
5 data transmission, routing, intermediate and tran-  
6 sient storage, or connections to its system or net-  
7 work, where the person providing such services does  
8 not select or modify the content of the electronic  
9 data, is not the sender or the intended recipient of  
10 the data, and does not differentiate personally iden-  
11 tifiable information from other information that  
12 such person transmits, routes, or stores, or for  
13 which such person provides connections. Any such  
14 person shall be treated as a service provider under  
15 this subtitle only to the extent that it is engaged in  
16 the provision of such transmission, routing, inter-  
17 mediate and transient storage, or connections.

18 **SEC. 142. NOTICE TO INDIVIDUALS.**

19 (a) IN GENERAL.—A covered entity that owns or pos-  
20 sesses data in electronic form containing personally identi-  
21 fiable information, following the discovery of a breach of  
22 security of the system maintained by the covered entity  
23 that contains such information, shall notify—

24 (1) each individual who is a citizen or resident  
25 of the United States and whose personally identifi-

1       able information has been, or is reasonably believed  
2       to have been, acquired or accessed from the covered  
3       entity as a result of the breach of security; and

4               (2) the Commission, unless the covered entity  
5       has notified the designated entity under section 143.

6       (b) SPECIAL NOTIFICATION REQUIREMENTS.—

7               (1) THIRD PARTIES.—In the event of a breach  
8       of security of a system maintained by a third party  
9       that has been contracted to maintain or process data  
10      in electronic form containing personally identifiable  
11      information on behalf of a covered entity who owns  
12      or possesses such data, the third party shall notify  
13      the covered entity of the breach of security.

14              (2) SERVICE PROVIDERS.—If a service provider  
15      becomes aware of a breach of security of data in  
16      electronic form containing personally identifiable in-  
17      formation that is owned or possessed by another cov-  
18      ered entity that connects to or uses a system or net-  
19      work provided by the service provider for the pur-  
20      pose of transmitting, routing, or providing inter-  
21      mediate or transient storage of such data, the serv-  
22      ice provider shall notify of the breach of security  
23      only the covered entity who initiated such connec-  
24      tion, transmission, routing, or storage if such cov-  
25      ered entity can be reasonably identified.

1           (3) COORDINATION OF NOTIFICATION WITH  
2 CREDIT REPORTING AGENCIES.—

3           (A) IN GENERAL.—If a covered entity is  
4 required to provide notification to more than  
5 5,000 individuals under subsection (a)(1), the  
6 covered entity also shall notify each major cred-  
7 it reporting agency of the timing and distribu-  
8 tion of the notices, except when the only per-  
9 sonally identifiable information that is the sub-  
10 ject of the breach of security is the individual's  
11 first name or initial and last name, or address,  
12 or phone number, in combination with a credit  
13 or debit card number, and any required security  
14 code.

15           (B) NOTICE TO CREDIT REPORTING AGEN-  
16 CIES BEFORE INDIVIDUALS.—Such notice shall  
17 be given to each credit reporting agency without  
18 unreasonable delay and, if it will not delay no-  
19 tice to the affected individuals, prior to the dis-  
20 tribution of notices to the affected individuals.

21 (c) TIMELINESS OF NOTIFICATION.—

22           (1) IN GENERAL.—All notifications required  
23 under this section shall be made without unreason-  
24 able delay following the discovery by the covered en-  
25 tity of a security breach.

1 (2) REASONABLE DELAY.—

2 (A) IN GENERAL.—Reasonable delay under  
3 this subsection may include any time necessary  
4 to determine the scope of the security breach,  
5 prevent further disclosures, restore the reason-  
6 able integrity of the data system, and provide  
7 notice to law enforcement when required.

8 (B) EXTENSION.—

9 (i) IN GENERAL.—Except as provided  
10 in subsection (d), delay of notification shall  
11 not exceed 60 days following the discovery  
12 of the security breach, unless the covered  
13 entity requests an extension of time and  
14 the Commission determines in writing that  
15 additional time is reasonably necessary to  
16 determine the scope of the security breach,  
17 prevent further disclosures, restore the rea-  
18 sonable integrity of the data system, or to  
19 provide notice to the designated entity.

20 (ii) APPROVAL OF REQUEST.—If the  
21 Commission approves the request for delay,  
22 the covered entity may delay the period for  
23 notification for additional periods of up to  
24 30 days.

1           (3) BURDEN OF PRODUCTION.—The covered  
 2           entity, third party, or service provider required to  
 3           provide notice under this title shall, upon the request  
 4           of the Commission provide records or other evidence  
 5           of the notifications required under this subtitle, in-  
 6           cluding to the extent applicable, the reasons for any  
 7           delay of notification.

8           (d) METHOD AND CONTENT OF NOTIFICATION.—

9           (1) DIRECT NOTIFICATION.—

10           (A) METHOD OF DIRECT NOTIFICATION.—

11           Except as provided in paragraph (2), a covered  
 12           entity shall be in compliance with the notifica-  
 13           tion requirement under subsection (a)(1) if—

14                   (i) the covered entity provides con-  
 15                   spicuous and clearly identified notifica-  
 16                   tion—

17                           (I) in writing; or

18                           (II) by e-mail or other electronic  
 19                   means if—

20                                   (aa) the covered entity's pri-  
 21                                   mary method of communication  
 22                                   with the individual is by e-mail or  
 23                                   such other electronic means; or

24                                   (bb) the individual has con-  
 25                                   sented to receive notification by

1 e-mail or such other electronic  
2 means and such notification is  
3 provided in a manner that is con-  
4 sistent with the provisions per-  
5 mitting electronic transmission of  
6 notices under section 101 of the  
7 Electronic Signatures in Global  
8 and National Commerce Act (15  
9 U.S.C. 7001); and

10 (ii) the method of notification selected  
11 under clause (i) can reasonably be expected  
12 to reach the intended individual.

13 (B) CONTENT OF DIRECT NOTIFICA-  
14 TION.—Each method of notification under sub-  
15 paragraph (A) shall include the following:

16 (i) The date, estimated date, or esti-  
17 mated date range of the breach of security.

18 (ii) A description of the personally  
19 identifiable information that was or is rea-  
20 sonably believed to have been acquired or  
21 accessed as a result of the breach of secu-  
22 rity.

23 (iii) A telephone number that an indi-  
24 vidual can use at no cost to the individual  
25 to contact the covered entity to inquire

1           about the breach of security or the infor-  
 2           mation the covered entity maintained  
 3           about that individual.

4           (iv) Notice that the individual may be  
 5           entitled to consumer credit reports under  
 6           subsection (e)(1).

7           (v) Instructions how an individual can  
 8           request consumer credit reports under sub-  
 9           section (e)(1).

10          (vi) A telephone number, that an indi-  
 11          vidual can use at no cost to the individual,  
 12          and an address to contact each major cred-  
 13          it reporting agency.

14          (vii) A telephone number, that an in-  
 15          dividual can use at no cost to the indi-  
 16          vidual, and an Internet website address to  
 17          obtain information regarding identity theft  
 18          from the Commission.

19          (2) SUBSTITUTE NOTIFICATION.—

20           (A) CIRCUMSTANCES GIVING RISE TO SUB-  
 21          STITUTE NOTIFICATION.—A covered entity re-  
 22          quired to provide notification to individuals  
 23          under subsection (a)(1) may provide notifica-  
 24          tion under this paragraph instead of paragraph  
 25          (1) of this subsection if—

1 (i) notification under paragraph (1) is  
2 not feasible due to lack of sufficient con-  
3 tact information for the individual required  
4 to be notified; or

5 (ii) the covered entity owns or pos-  
6 sesses data in electronic form containing  
7 personally identifiable information of fewer  
8 than 10,000 individuals and direct notifica-  
9 tion is not feasible due to excessive cost to  
10 the covered entity required to provide such  
11 notification relative to the resources of  
12 such covered entity, as determined in ac-  
13 cordance with the regulations issued by the  
14 Commission under paragraph (3)(A).

15 (B) METHOD OF SUBSTITUTE NOTIFICA-  
16 TION.—Notification under this paragraph shall  
17 include the following:

18 (i) Conspicuous and clearly identified  
19 notification by e-mail to the extent the cov-  
20 ered entity has an e-mail address for an in-  
21 dividual who is entitled to notification  
22 under subsection (a)(1).

23 (ii) Conspicuous and clearly identified  
24 notification on the Internet website of the

covered entity if the covered entity maintains an Internet website.

(iii) Notification to print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personally identifiable information was acquired or accessed reside.

(C) CONTENT OF SUBSTITUTE NOTIFICATION.—Each method of notification under this paragraph shall include the following:

(i) The date, estimated date, or estimated date range of the breach of security.

(ii) A description of the types of personally identifiable information that were or are reasonably believed to have been acquired or accessed as a result of the breach of security.

(iii) Notice that an individual may be entitled to consumer credit reports under subsection (e)(1).

(iv) Instructions how an individual can request consumer credit reports under subsection (e)(1).

(v) A telephone number that an individual can use at no cost to the individual

1 to learn whether the individual's personally  
2 identifiable information is included in the  
3 breach of security.

4 (vi) A telephone number, that an indi-  
5 vidual can use at no cost to the individual,  
6 and an address to contact each major cred-  
7 it reporting agency.

8 (vii) A telephone number, that an in-  
9 dividual can use at no cost to the indi-  
10 vidual, and an Internet website address to  
11 obtain information from the Commission  
12 regarding identity theft.

13 (3) REGULATIONS AND GUIDANCE.—

14 (A) REGULATIONS CONCERNING SUB-  
15STITUTE NOTIFICATION.—

16 (i) IN GENERAL.—Not later than 1  
17 year after the date of enactment of this  
18 Act, the Commission shall prescribe cri-  
19 teria for determining circumstances under  
20 which notification may be provided under  
21 paragraph (2), including criteria for deter-  
22 mining whether providing notification  
23 under paragraph (1) is not feasible due to  
24 excessive costs to the covered entity re-

1           quired to provide such notification relative  
2           to the resources of such covered entity.

3           (ii) OTHER CIRCUMSTANCES.—The  
4           regulations required by clause (i) may also  
5           identify other circumstances in which noti-  
6           fication under paragraph (2) would be ap-  
7           propriate, including circumstances under  
8           which the cost of providing direct notifica-  
9           tion exceeds the benefits to individuals.

10          (B) GUIDANCE.—

11           (i) IN GENERAL.—The Commission, in  
12           consultation with the Administrator of the  
13           Small Business Administration, shall pub-  
14           lish and otherwise make available general  
15           guidance with respect to compliance with  
16           this subsection.

17           (ii) CONTENTS.—The guidance re-  
18           quired by clause (i) shall include the fol-  
19           lowing:

20                   (I) A description of written or e-  
21                   mail notification that complies with  
22                   paragraph (1).

23                   (II) Guidance on the content of  
24                   notification under paragraph (2), in-  
25                   cluding the extent of notification to

1 print and broadcast media that com-  
2 plies with subparagraph (B)(iii) of  
3 such paragraph.

4 (e) OTHER OBLIGATIONS FOLLOWING BREACH.—

5 (1) IN GENERAL.—Subject to the provisions of  
6 this subsection, not later than 60 days after the date  
7 of a request by an individual who received notifica-  
8 tion under subsection (a)(1) and quarterly thereafter  
9 for 2 years, a covered entity required to provide no-  
10 tification under such subsection to such individual  
11 shall provide, or arrange for the provision of, to such  
12 individual at no cost to such individual, consumer  
13 credit reports from at least 1 major credit reporting  
14 agency.

15 (2) LIMITATION.—Paragraph (1) shall not  
16 apply if the only personally identifiable information  
17 that is the subject of the breach of security is the  
18 individual's first name or initial and last name, or  
19 address, or phone number, in combination with a  
20 credit or debit card number, and any required secu-  
21 rity code.

22 (3) RULEMAKING.—Not later than 1 year after  
23 the date of enactment of this Act, the Commission  
24 shall prescribe the following:

1           (A) Criteria for determining the cir-  
2           cumstances under which a covered entity re-  
3           quired to provide notification under subsection  
4           (a)(1) must provide or arrange for the provision  
5           of free consumer credit reports under this sub-  
6           section.

7           (B) A simple process under which a cov-  
8           ered entity that is a small business concern or  
9           small nonprofit organization may request a full  
10          or a partial waiver or a modified or an alter-  
11          native means of complying with this subsection  
12          if providing free consumer credit reports is not  
13          feasible due to excessive costs relative to the re-  
14          sources of such covered entity and relative to  
15          the level of harm, to affected individuals,  
16          caused by the breach of security.

17       (4) DEFINITIONS.—In this subsection:

18           (A) SMALL BUSINESS CONCERN.—The  
19           term “small business concern” has the meaning  
20           given such term under section 3 of the Small  
21           Business Act (15 U.S.C. 632).

22           (B) SMALL NONPROFIT ORGANIZATION.—  
23           The term “small nonprofit organization” has  
24           the meaning the Commission shall give such  
25           term for purposes of this subsection.

1 (f) DELAY OF NOTIFICATION AUTHORIZED FOR NA-  
2 TIONAL SECURITY AND LAW ENFORCEMENT PUR-  
3 POSES.—

4 (1) IN GENERAL.—If the United States Secret  
5 Service or the Federal Bureau of Investigation de-  
6 termines that notification under this section would  
7 impede a criminal investigation or a national secu-  
8 rity activity, such notification shall be delayed upon  
9 written notice from the United States Secret Service  
10 or the Federal Bureau of Investigation to the cov-  
11 ered entity that experienced the breach of security.  
12 The notification from the United States Secret Serv-  
13 ice or the Federal Bureau of Investigation shall  
14 specify the period of delay requested for national se-  
15 curity or law enforcement purposes.

16 (2) SUBSEQUENT DELAY OF NOTIFICATION.—

17 (A) IN GENERAL.—If the notification re-  
18 quired under subsection (a)(1) is delayed pursu-  
19 ant to paragraph (1), a covered entity shall give  
20 notice not more than 30 days after the day  
21 such law enforcement or national security delay  
22 was invoked unless a Federal law enforcement  
23 or intelligence agency provides written notifica-  
24 tion that further delay is necessary.

1 (B) WRITTEN JUSTIFICATION REQUIRE-  
2 MENTS.—

3 (i) UNITED STATES SECRET SERV-  
4 ICE.—If the United States Secret Service  
5 instructs a covered entity to delay notifica-  
6 tion under this section beyond the 30-day  
7 period set forth in subparagraph (A) (re-  
8 ferred to in this clause as “subsequent  
9 delay”), the United States Secret Service  
10 shall submit written justification for the  
11 subsequent delay to the Secretary of  
12 Homeland Security before the subsequent  
13 delay begins.

14 (ii) FEDERAL BUREAU OF INVESTIGA-  
15 TION.—If the Federal Bureau of Investiga-  
16 tion instructs a covered entity to delay no-  
17 tification under this section beyond the 30-  
18 day period set forth in subparagraph (A)  
19 (referred to in this clause as “subsequent  
20 delay”), the Federal Bureau of Investiga-  
21 tion shall submit written justification for  
22 the subsequent delay to the Attorney Gen-  
23 eral before the subsequent delay begins.

24 (3) LAW ENFORCEMENT IMMUNITY.—No cause  
25 of action shall lie in any court against any Federal

1 agency for acts relating to the delay of notification  
2 for national security or law enforcement purposes  
3 under this subtitle.

4 (g) GENERAL EXEMPTION.—

5 (1) IN GENERAL.—A covered entity shall be ex-  
6 empt from the requirements under this section if,  
7 following a breach of security, the covered entity  
8 reasonably concludes that there is no reasonable risk  
9 of identity theft, fraud, or other unlawful conduct.

10 (2) FTC GUIDANCE.—Not later than 1 year  
11 after the date of enactment of this Act, the Commis-  
12 sion, after consultation with the Director of the Na-  
13 tional Institute of Standards and Technology, shall  
14 issue guidance regarding the application of the ex-  
15 emption under paragraph (1).

16 (h) EXEMPTIONS FOR NATIONAL SECURITY AND  
17 LAW ENFORCEMENT PURPOSES.—

18 (1) IN GENERAL.—A covered entity shall be ex-  
19 empt from the notice requirements under this sec-  
20 tion if—

21 (A) a determination is made—

22 (i) by the United States Secret Serv-  
23 ice or the Federal Bureau of Investigation  
24 that notification of the breach of security  
25 could be reasonably expected to reveal sen-

1           sitive sources and methods or similarly im-  
2           pede the ability of the Government to con-  
3           duct law enforcement or intelligence inves-  
4           tigations; or

5           (ii) by the Federal Bureau of Inves-  
6           tigation that notification of the breach of  
7           security could be reasonably expected to  
8           cause damage to the national security; and

9           (B) the United States Secret Service or the  
10          Federal Bureau of Investigation, as the case  
11          may be, provides written notice of its deter-  
12          mination under subparagraph (A) to the cov-  
13          ered entity.

14          (2) UNITED STATES SECRET SERVICE.—If the  
15          United States Secret Service invokes an exemption  
16          under paragraph (1), the United States Secret Serv-  
17          ice shall submit written justification for invoking the  
18          exemption to the Secretary of Homeland Security  
19          before the exemption is invoked.

20          (3) FEDERAL BUREAU OF INVESTIGATION.—If  
21          the Federal Bureau of Investigation invokes an ex-  
22          emption under paragraph (1), the Federal Bureau of  
23          Investigation shall submit written justification for  
24          invoking the exemption to the Attorney General be-  
25          fore the exemption is invoked.

1           (4) IMMUNITY.—No cause of action shall lie in  
 2           any court against any Federal agency for acts relat-  
 3           ing to the exemption from notification for national  
 4           security or law enforcement purposes under this sub-  
 5           title.

6           (5) REPORTS.—Not later than 540 days after  
 7           the date of enactment of this Act, and upon request  
 8           by Congress thereafter, the United States Secret  
 9           Service and the Federal Bureau of Investigation  
 10          shall submit to Congress a report on the number  
 11          and nature of breaches of security subject to the ex-  
 12          emptions for national security and law enforcement  
 13          purposes under this subsection.

14          (i) FINANCIAL FRAUD PREVENTION EXEMPTION.—

15               (1) IN GENERAL.—A covered entity shall be ex-  
 16               empt from the notice requirements under this sec-  
 17               tion if the covered entity utilizes or participates in  
 18               a security program that—

19                       (A) effectively blocks the use of the person-  
 20                       ally identifiable information to initiate an unau-  
 21                       thorized financial transaction before it is  
 22                       charged to the account of the individual; and

23                       (B) provides notice to each affected indi-  
 24                       vidual after a breach of security that resulted in

1 attempted fraud or an attempted unauthorized  
2 transaction.

3 (2) LIMITATIONS.—An exemption under para-  
4 graph (1) shall not apply if—

5 (A) the breach of security includes person-  
6 ally identifiable information, other than a credit  
7 card number or credit card security code, of  
8 any type; or

9 (B) the breach of security includes both  
10 the individual's credit card number and the in-  
11 dividual's first and last name.

12 (j) FINANCIAL INSTITUTIONS REGULATED BY FED-  
13 ERAL FUNCTIONAL REGULATORS.—

14 (1) IN GENERAL.—A covered financial institu-  
15 tion shall be deemed in compliance with this section  
16 if—

17 (A) the Federal functional regulator with  
18 jurisdiction over the covered financial institu-  
19 tion has issued a standard by regulation or  
20 guideline under title V of the Gramm-Leach-  
21 Bliley Act (15 U.S.C. 6801 et seq.) that—

22 (i) requires financial institutions with-  
23 in its jurisdiction to provide notification to  
24 individuals following a breach of security;  
25 and

1 (ii) provides protections substantially  
 2 similar to, or greater than, those required  
 3 under this Act; and

4 (B) the covered financial institution is in  
 5 compliance with the standard under subpara-  
 6 graph (A).

7 (2) DEFINITIONS.—In this subsection:

8 (A) COVERED FINANCIAL INSTITUTION.—  
 9 The term “covered financial institution” means  
 10 a financial institution that is subject to—

11 (i) the data security requirements of  
 12 the Gramm-Leach-Bliley Act (15 U.S.C.  
 13 6801 et seq.);

14 (ii) any implementing standard issued  
 15 by regulation or guideline issued under  
 16 that Act; and

17 (iii) the jurisdiction of a Federal func-  
 18 tional regulator under that Act.

19 (B) FEDERAL FUNCTIONAL REGULATOR.—  
 20 The term “Federal functional regulator” has  
 21 the meaning given the term in section 509 of  
 22 the Gramm-Leach-Bliley Act (15 U.S.C. 6809).

23 (C) FINANCIAL INSTITUTION.—The term  
 24 “financial institution” has the meaning given

1           the term in section 509 of the Gramm-Leach-  
2           Bliley Act (15 U.S.C. 6809).

3       (k) EXEMPTION; HEALTH PRIVACY.—

4           (1) COVERED ENTITY OR BUSINESS ASSOCIATE  
5       UNDER HITECH ACT.—To the extent that a covered  
6       entity under this section acts as a covered entity or  
7       a business associate under section 13402 of the  
8       Health Information Technology for Economic and  
9       Clinical Health Act (42 U.S.C. 17932), has the obli-  
10      gation to provide notification to individuals following  
11      a breach of security under that Act or its imple-  
12      menting regulations, and is in compliance with that  
13      obligation, the covered entity shall be deemed in  
14      compliance with this section.

15          (2) ENTITY SUBJECT TO HITECH ACT.—To the  
16      extent that a covered entity under this section acts  
17      as a vendor of personal health records, a third party  
18      service provider, or other entity subject to section  
19      13407 of the Health Information Technology for Ec-  
20      onomical and Clinical Health Act (42 U.S.C.  
21      17937), has the obligation to provide notification to  
22      individuals following a breach of security under that  
23      Act or its implementing regulations, and is in com-  
24      pliance with that obligation, the covered entity shall  
25      be deemed in compliance with this section.

1           (3) LIMITATION OF STATUTORY CONSTRUC-  
 2           TION.—Nothing in this subtitle may be construed in  
 3           any way to give effect to the sunset provision under  
 4           section 13407(g)(2) of the Health Information Tech-  
 5           nology for Economic and Clinical Health Act (42  
 6           U.S.C. 17937(g)(2)) or to otherwise limit or affect  
 7           the applicability, under section 13407 of that Act, of  
 8           the requirement to provide notification to individuals  
 9           following a breach of security for vendors of personal  
 10          health records and each entity described in clause  
 11          (ii), (iii), or (iv) of section 13424(b)(1)(A) of that  
 12          Act (42 U.S.C. 17953(b)(1)(A)).

13          (l) INTERNET WEBSITE NOTICE OF FEDERAL TRADE  
 14          COMMISSION.—If the Commission, upon receiving notifi-  
 15          cation of any breach of security that is reported to the  
 16          Commission, finds that notification of the breach of secu-  
 17          rity via the Commission’s Internet website would be in the  
 18          public interest or for the protection of consumers, the  
 19          Commission shall place such a notice in a clear and con-  
 20          spicuous location on its Internet website.

21          (m) FTC STUDY ON NOTIFICATION IN LANGUAGES  
 22          IN ADDITION TO ENGLISH.—Not later than 1 year after  
 23          the date of enactment of this Act, the Commission shall  
 24          conduct a study on the feasibility and advisability of re-  
 25          quiring notification provided pursuant to subsection (d)(1)

1 to be provided in a language in addition to English to indi-  
2 viduals known to speak only such other language.

3 **SEC. 143. NOTICE TO LAW ENFORCEMENT.**

4 (a) DESIGNATION OF GOVERNMENT ENTITY TO RE-  
5 CEIVE NOTICE.—Not later than 60 days after the date  
6 of enactment of this Act, the Secretary of Homeland Secu-  
7 rity shall designate a Federal Government entity to receive  
8 notice under this section.

9 (b) NOTICE TO DESIGNATED ENTITY.—A covered en-  
10 tity shall notify the designated entity of a breach of secu-  
11 rity if—

12 (1) the number of individuals whose personally  
13 identifiable information was, or is reasonably be-  
14 lieved to have been, acquired or accessed as a result  
15 of the breach of security exceeds 10,000;

16 (2) the breach of security involves a database,  
17 networked or integrated databases, or other data  
18 system containing the personally identifiable infor-  
19 mation of more than 1,000,000 individuals;

20 (3) the breach of security involves databases  
21 owned by the Federal Government; or

22 (4) the breach of security involves primarily  
23 personally identifiable information of individuals  
24 known to the covered entity to be employees or con-

1 tractors of the Federal Government involved in na-  
2 tional security or law enforcement.

3 (c) CONTENT OF NOTICES.—

4 (1) IN GENERAL.—Each notice under sub-  
5 section (b) shall contain the following:

6 (A) The date, estimated date, or estimated  
7 date range of the breach of security.

8 (B) A description of the nature of the  
9 breach of security.

10 (C) A description of each type of person-  
11 ally identifiable information that was or is rea-  
12 sonably believed to have been acquired or  
13 accessed as a result of the breach of security.

14 (D) A statement of each paragraph under  
15 subsection (b) that applies to the breach of se-  
16 curity.

17 (2) CONSTRUCTION.—Nothing in this section  
18 shall be construed to require a covered entity to re-  
19 veal specific or identifying information about an in-  
20 dividual as part of the notice under paragraph (1).

21 (d) NOTICE BY DESIGNATED ENTITY.—The des-  
22 ignated entity shall promptly provide each notice it re-  
23 ceives under subsection (b) to the following:

24 (1) The United States Secret Service.

25 (2) The Federal Bureau of Investigation.

1           (3) The Commission.

2           (4) The United States Postal Inspection Serv-  
3       ice, if the breach of security involves mail fraud.

4           (5) The attorney general of each State affected  
5       by the breach of security.

6           (6) Such other Federal agencies as the des-  
7       ignated entity considers appropriate for law enforce-  
8       ment, national security, or data security purposes.

9       (e) TIMING OF NOTICES.—Notice under this section  
10   shall be delivered as follows:

11           (1) Notice under subsection (b) shall be deliv-  
12       ered as promptly as possible, but—

13                (A) not less than 3 business days before  
14       notification to an individual section 142(a)(1);  
15       and

16                (B) not later than 10 days after the date  
17       of discovery of the events requiring notice.

18           (2) Notice under subsection (d) shall be deliv-  
19       ered as promptly as possible, but not later than 1  
20       business day after the date that the designated enti-  
21       ty receives notice of a breach of security from a cov-  
22       ered entity.

## **Subtitle E—Enforcement**

### **2 SEC. 151. GENERAL APPLICATION.**

3       The requirements of this title shall apply to any per-  
4 son who—

5           (1) collects, uses, transfers, or stores covered  
6 information concerning more than 5,000 individuals  
7 during any consecutive 12-month period; and

8           (2) is—

9           (A) a person over which the Commission  
10 has authority pursuant to section 5(a)(2) of the  
11 Federal Trade Commission Act (15 U.S.C.  
12 45(a)(2));

13           (B) a common carrier subject to the Com-  
14 munications Act of 1934 (47 U.S.C. 151 et  
15 seq.), notwithstanding the definition of the term  
16 “Acts to regulate commerce” in section 4 of the  
17 Federal Trade Commission Act (15 U.S.C. 44)  
18 and the exception provided by section 5(a)(2) of  
19 the Federal Trade Commission Act (15 U.S.C.  
20 45(a)(2)) for such carriers; or

21           (C) a nonprofit organization, including any  
22 organization described in section 501(c) of the  
23 Internal Revenue Code of 1986 that is exempt  
24 from taxation under section 501(a) of such  
25 Code, notwithstanding the definition of the

1 term “Acts to regulate commerce” in section 4  
 2 of the Federal Trade Commission Act (15  
 3 U.S.C. 44) and the exception provided by sec-  
 4 tion 5(a)(2) of the Federal Trade Commission  
 5 Act (15 U.S.C. 45(a)(2)) for such organiza-  
 6 tions.

7 **SEC. 152. ENFORCEMENT BY THE FEDERAL TRADE COM-**  
 8 **MISSION.**

9 (a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—  
 10 A reckless or repetitive violation of a provision of this title,  
 11 except section 143, shall be treated as an unfair or decep-  
 12 tive act or practice in violation of a regulation under sec-  
 13 tion 18(a)(1)(B) of the Federal Trade Commission Act  
 14 (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive  
 15 acts or practices.

16 (b) POWERS OF COMMISSION.—

17 (1) IN GENERAL.—Except as provided in para-  
 18 graph (3), the Commission shall enforce this title,  
 19 except section 143, in the same manner, by the same  
 20 means, and with the same jurisdiction, powers, and  
 21 duties as though all applicable terms and provisions  
 22 of the Federal Trade Commission Act (15 U.S.C. 41  
 23 et seq.) were incorporated into and made a part of  
 24 this title.

1           (2) PRIVILEGES AND IMMUNITIES.—Except as  
2       provided in paragraph (3), any person who violates  
3       a provision of this title, except section 143, shall be  
4       subject to the penalties and entitled to the privileges  
5       and immunities provided in the Federal Trade Com-  
6       mission Act (15 U.S.C. 41 et seq.).

7           (3) COMMON CARRIERS AND NONPROFIT ORGA-  
8       NIZATIONS.—The Commission shall enforce this  
9       title, except section 143, with respect to common  
10      carriers and nonprofit organizations described in  
11      section 151 to the extent necessary to effectuate the  
12      purposes of this title as if such carriers and non-  
13      profit organizations were persons over which the  
14      Commission has authority pursuant to section  
15      5(a)(2) of the Federal Trade Commission Act (15  
16      U.S.C. 45(a)(2)).

17      (c) RULEMAKING AUTHORITY.—

18           (1) LIMITATION.—In promulgating rules under  
19      this title, the Commission may not require the de-  
20      ployment or use of any specific products or tech-  
21      nologies, including any specific computer software or  
22      hardware.

23           (2) ADMINISTRATIVE PROCEDURE.—The Com-  
24      mission shall promulgate regulations under this title

1 in accordance with section 553 of title 5, United  
2 States Code.

3 (d) RULE OF CONSTRUCTION.—Nothing in this title  
4 shall be construed to limit the authority of the Commission  
5 under any other provision of law.

6 **SEC. 153. ENFORCEMENT BY ATTORNEY GENERAL.**

7 (a) IN GENERAL.—The Attorney General may bring  
8 a civil action in the appropriate United States district  
9 court against any covered entity that engages in conduct  
10 constituting a violation of section 143.

11 (b) PENALTIES.—

12 (1) IN GENERAL.—Upon proof of such conduct  
13 by a preponderance of the evidence, a covered entity  
14 shall be subject to a civil penalty of not more than  
15 \$1,000 per individual whose personally identifiable  
16 information was or is reasonably believed to have  
17 been accessed or acquired as a result of the breach  
18 of security that is the basis of the violation, up to  
19 a maximum of \$100,000 per day while such violation  
20 persists.

21 (2) LIMITATIONS.—The total amount of the  
22 civil penalty assessed under this subsection against  
23 a covered entity for acts or omissions relating to a  
24 single breach of security shall not exceed  
25 \$3,000,000, unless the conduct constituting a viola-

1       tion of subtitle D was reckless or repeated, in which  
 2       case an additional civil penalty of up to \$3,000,000  
 3       may be imposed.

4           (3) ADJUSTMENT FOR INFLATION.—Beginning  
 5       on the date that the Consumer Price Index is first  
 6       published by the Bureau of Labor Statistics that is  
 7       after 1 year after the date of enactment of this Act,  
 8       and each year thereafter, the amounts specified in  
 9       paragraphs (1) and (2) shall be increased by the  
 10      percentage increase in the Consumer Price Index  
 11      published on that date from the Consumer Price  
 12      Index published the previous year.

13      (c) INJUNCTIVE ACTIONS.—If it appears that a cov-  
 14      ered entity has engaged, or is engaged, in any act or prac-  
 15      tice that constitutes a violation of subtitle D, the Attorney  
 16      General may petition an appropriate United States district  
 17      court for an order enjoining such practice or enforcing  
 18      compliance with such subtitle.

19      (d) ISSUANCE OF ORDER.—A court may issue such  
 20      an order under paragraph (c) if it finds that the conduct  
 21      in question constitutes a violation of subtitle D.

22   **SEC. 154. ENFORCEMENT BY STATES.**

23      (a) CIVIL ACTION.—In any case in which the attor-  
 24      ney general of a State has reason to believe that an inter-  
 25      est of the residents of that State has been or is adversely

1 affected by a covered entity who violates any part of this  
 2 title in a manner that results in economic or physical harm  
 3 to an individual or engages in a pattern or practice that  
 4 violates any part of this title other than section 143, the  
 5 attorney general may, as *parens patriae*, bring a civil ac-  
 6 tion on behalf of the residents of the State in an appro-  
 7 priate district court of the United States—

8 (1) to enjoin further violation of this title or a  
 9 regulation promulgated under this title by the de-  
 10 fendant;

11 (2) to compel compliance with this title or a  
 12 regulation promulgated under this title; or

13 (3) for violations of this title or a regulation  
 14 promulgated under this title to obtain civil penalties  
 15 in the amount determined under section title.

16 (b) RIGHTS OF FEDERAL TRADE COMMISSION.—

17 (1) NOTICE TO FEDERAL TRADE COMMIS-  
 18 SION.—

19 (A) IN GENERAL.—Except as provided in  
 20 subparagraph (C), the attorney general of a  
 21 State shall notify the Commission in writing of  
 22 any civil action under subsection (b), prior to  
 23 initiating such civil action.

24 (B) CONTENTS.—The notice required by  
 25 subparagraph (A) shall include a copy of the

1 complaint to be filed to initiate such civil ac-  
2 tion.

3 (C) EXCEPTION.—If it is not feasible for  
4 the attorney general of a State to provide the  
5 notice required by subparagraph (A), the State  
6 shall provide notice immediately upon insti-  
7 tuting a civil action under subsection (b).

8 (2) INTERVENTION BY FEDERAL TRADE COM-  
9 MISSION.—Upon receiving notice required by para-  
10 graph (1) with respect to a civil action, the Commis-  
11 sion may—

12 (A) intervene in such action; and

13 (B) upon intervening—

14 (i) be heard on all matters arising in  
15 such civil action; and

16 (ii) file petitions for appeal of a deci-  
17 sion in such action.

18 (c) PREEMPTIVE ACTION BY FEDERAL TRADE COM-  
19 MISSION.—If the Commission institutes a civil action for  
20 violation of this title or a regulation promulgated under  
21 this title, no attorney general of a State may bring a civil  
22 action under subsection (a) against any defendant named  
23 in the complaint of the Commission for violation of this  
24 title or a regulation promulgated under this title that is  
25 alleged in such complaint.

1 (d) INVESTIGATORY POWERS.—Nothing in this sec-  
 2 tion may be construed to prevent the attorney general of  
 3 a State from exercising the powers conferred on such at-  
 4 torney general by the laws of such State to conduct inves-  
 5 tigation or to administer oaths or affirmations or to com-  
 6 pel the attendance of witnesses or the production of docu-  
 7 mentary and other evidence.

8 (e) VENUE; SERVICE OF PROCESS.—

9 (1) VENUE.—Any action brought under sub-  
 10 section (a) may be brought in—

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

15 (B) another court of competent jurisdic-  
 16 tion.

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

20 (A) is an inhabitant; or

21 (B) may be found.

22 (f) ACTIONS BY OTHER STATE OFFICIALS.—

23 (1) IN GENERAL.—In addition to civil actions  
 24 brought by attorneys general under subsection (a),  
 25 any other officer of a State who is authorized by the

1 State to do so may bring a civil action under sub-  
 2 section (a), subject to the same requirements and  
 3 limitations that apply under this section to civil ac-  
 4 tions brought by attorneys general.

5 (2) SAVINGS PROVISION.—Nothing in this sec-  
 6 tion may be construed to prohibit an authorized offi-  
 7 cial of a State from initiating or continuing any pro-  
 8 ceeding in a court of the State for a violation of any  
 9 civil or criminal law of the State.

10 **SEC. 155. CIVIL PENALTIES.**

11 (a) IN GENERAL.—In an action brought under sec-  
 12 tion 154, in addition to any other penalty otherwise appli-  
 13 cable to a violation of this title or any regulation promul-  
 14 gated under this title, the following civil penalties shall  
 15 apply:

16 (1) SUBTITLE A VIOLATIONS.—A covered entity  
 17 that recklessly or repeatedly violates subtitle A is lia-  
 18 ble for a civil penalty equal to the amount calculated  
 19 by multiplying the number of days that the entity is  
 20 not in compliance with such subtitle by an amount  
 21 not to exceed \$33,000.

22 (2) SUBTITLE B VIOLATIONS.—A covered entity  
 23 that recklessly or repeatedly violates subtitle B is  
 24 liable for a civil penalty equal to the amount cal-  
 25 culated by multiplying the number of days that such

1       an entity is not in compliance with such subtitle, or  
2       the number of individuals for whom the entity failed  
3       to obtain consent as required by such subtitle,  
4       whichever is greater, by an amount not to exceed  
5       \$33,000.

6           (3) SUBTITLE D VIOLATIONS.—A covered entity  
7       that recklessly or repeatedly violates section 142 is  
8       liable for a civil penalty equal to the amount cal-  
9       culated by multiplying the number of violations of  
10      such section by an amount not to exceed \$33,000.  
11      Each failure to send notification as required under  
12      such section to a resident of the State shall be treat-  
13      ed as a separate violation.

14      (b) ADJUSTMENT FOR INFLATION.—Beginning on  
15      the date that the Consumer Price Index for All Urban  
16      Consumers is first published by the Bureau of Labor Sta-  
17      tistics that is after 1 year after the date of enactment of  
18      this Act, and each year thereafter, each of the amounts  
19      specified in subsection (a) shall be increased by the per-  
20      centage increase in the Consumer Price Index published  
21      on that date from the Consumer Price Index published  
22      the previous year.

23      (c) MAXIMUM TOTAL LIABILITY.—Notwithstanding  
24      the number of actions which may be brought against a  
25      covered entity under section 154, the maximum civil pen-

1 alty for which any covered entity may be liable under this  
 2 section in such actions shall not exceed—

3 (1) \$6,000,000 for any related series of viola-  
 4 tions of any rule promulgated under subtitle A;

5 (2) \$6,000,000 for any related series of viola-  
 6 tions of subtitle B; and

7 (3) \$6,000,000 for any related series of viola-  
 8 tions of section 142.

9 **SEC. 156. EFFECT ON OTHER LAWS.**

10 (a) **PREEMPTION OF STATE LAWS.**—The provisions  
 11 of this title shall supersede any provisions of the law of  
 12 any State relating to those entities covered by the regula-  
 13 tions issued pursuant to this title, to the extent that such  
 14 provisions relate to the collection, use, or disclosure of—

15 (1) covered information addressed in this title;

16 or

17 (2) personally identifiable information or per-  
 18 sonal identification information addressed in provi-  
 19 sions of the law of a State.

20 (b) **UNAUTHORIZED CIVIL ACTIONS; CERTAIN STATE**  
 21 **LAWS.**—

22 (1) **UNAUTHORIZED ACTIONS.**—No person  
 23 other than a person specified in section 154 may  
 24 bring a civil action under the laws of any State if  
 25 such action is premised in whole or in part upon the

1 defendant violating this title or a regulation promul-  
 2 gated under this title.

3 (2) PROTECTION OF CERTAIN STATE LAWS.—

4 This title shall not be construed to preempt the ap-  
 5 plicability of—

6 (A) State laws that address the collection,  
 7 use, or disclosure of health information or fi-  
 8 nancial information; or

9 (B) other State laws to the extent that  
 10 those laws relate to acts of fraud.

11 (c) RULE OF CONSTRUCTION RELATING TO RE-  
 12 QUIRED DISCLOSURES TO GOVERNMENT ENTITIES.—

13 This title shall not be construed to expand or limit the  
 14 duty or authority of a covered entity or third party to dis-  
 15 close personally identifiable information to a Government  
 16 entity under any provision of law.

17 **SEC. 157. NO PRIVATE RIGHT OF ACTION.**

18 This title may not be construed to provide any private  
 19 right of action.

## 20 **Subtitle F—Co-Regulatory Safe** 21 **Harbor Programs**

22 **SEC. 161. ESTABLISHMENT OF SAFE HARBOR PROGRAMS.**

23 (a) IN GENERAL.—Not later than 1 year after the  
 24 date of enactment of this Act, the Commission shall ini-  
 25 tiate a rulemaking proceeding to establish requirements

1 for the establishment and administration of safe harbor  
 2 programs under which a nongovernmental organization  
 3 will administer a program that—

4 (1) establishes a mechanism for participants to  
 5 implement the requirements of this title with regards  
 6 to—

7 (A) certain types of unauthorized uses of  
 8 covered information as described in paragraph  
 9 (2); or

10 (B) any unauthorized use of covered infor-  
 11 mation; and

12 (2) offers consumers a clear, conspicuous, per-  
 13 sistent, and effective means of opting out of the  
 14 transfer of covered information by a covered entity  
 15 participating in the safe harbor program to a third  
 16 party for—

17 (A) behavioral advertising purposes;

18 (B) location-based advertising purposes;

19 (C) other specific types of unauthorized  
 20 use; or

21 (D) any unauthorized use.

22 (b) SELECTION OF NONGOVERNMENTAL ORGANIZA-  
 23 TIONS TO ADMINISTER PROGRAM.—

24 (1) SUBMITTAL OF APPLICATIONS.—An appli-  
 25 cant seeking to administer a program under the re-

1        requirements established pursuant to subsection (a)  
2        shall submit to the Commission an application there-  
3        for at such time, in such manner, and containing  
4        such information as the Commission may require.

5            (2) NOTICE AND RECEIPT OF APPLICATIONS.—

6        Upon completion of the rulemaking proceedings re-  
7        quired by subsection (a), the Commission shall—

8            (A) publish a notice in the Federal Reg-  
9            ister that it will receive applications for ap-  
10          proval of safe harbor programs under this sub-  
11          title; and

12          (B) begin receiving applications under  
13          paragraph (1).

14          (3) SELECTION.—Not later than 270 days after  
15          the date on which the Commission receives a com-  
16          pleted application under this subsection, the Com-  
17          mission shall grant or deny the application on the  
18          basis of the Commission’s evaluation of the appli-  
19          cant’s capacity to provide protection of individuals’  
20          covered information with regard to specific types of  
21          unauthorized uses of covered information as de-  
22          scribed in subsection (a)(2) that is substantially  
23          equivalent to or superior to the protection otherwise  
24          provided under this title.

1           (4) WRITTEN FINDINGS.—Any decision reached  
2       by the Commission under this subsection shall be ac-  
3       companied by written findings setting forth the basis  
4       for and reasons supporting such decision.

5       (c) SCOPE OF SAFE HARBOR PROTECTION.—The  
6       scope of protection offered by safe harbor programs ap-  
7       proved by the Commission that establish mechanisms for  
8       participants to implement the requirements of the title  
9       only for certain uses of covered information as described  
10      in subsection (a)(2) shall be limited to participating enti-  
11      ties' use of those particular types of covered information.

12      (d) SUPERVISION BY FEDERAL TRADE COMMIS-  
13      SION.—

14           (1) IN GENERAL.—The Commission shall exer-  
15      cise oversight and supervisory authority of a safe  
16      harbor program approved under this section  
17      through—

18           (A) ongoing review of the practices of the  
19           nongovernmental organization administering  
20           the program;

21           (B) the imposition of civil penalties on the  
22           nongovernmental organization if it is not com-  
23           pliant with the requirements established under  
24           subsection (a); and

1 (C) withdrawal of authorization to admin-  
2 ister the safe harbor program under this sub-  
3 title.

4 (2) ANNUAL REPORTS BY NONGOVERNMENTAL  
5 ORGANIZATIONS.—Each year, each nongovernmental  
6 organization administering a safe harbor program  
7 under this section shall submit to the Commission a  
8 report on its activities under this subtitle during the  
9 preceding year.

10 **SEC. 162. PARTICIPATION IN SAFE HARBOR PROGRAM.**

11 (a) EXEMPTION.—Any covered entity that partici-  
12 pates in, and demonstrates compliance with, a safe harbor  
13 program administered under section 161 shall be exempt  
14 from any provision of subtitle B or subtitle C if the Com-  
15 mission finds that the requirements of the safe harbor pro-  
16 gram are substantially the same as or more protective of  
17 privacy of individuals than the requirements of the provi-  
18 sion from which the exemption is granted.

19 (b) LIMITATION.—Nothing in this subtitle shall be  
20 construed to exempt any covered entity participating in  
21 a safe harbor program from compliance with any other  
22 requirement of the regulations promulgated under this  
23 title for which the safe harbor does not provide an excep-  
24 tion.

1 **Subtitle G—Application With Other**  
2 **Federal Laws**

3 **SEC. 171. APPLICATION WITH OTHER FEDERAL LAWS.**

4 (a) QUALIFIED EXEMPTION FOR PERSONS SUBJECT  
5 TO OTHER FEDERAL PRIVACY LAWS.—If a person is sub-  
6 ject to a provision of this title and a provision of a Federal  
7 privacy law described in subsection (d), such provision of  
8 this title shall not apply to such person to the extent that  
9 such provision of Federal privacy law applies to such per-  
10 son.

11 (b) PROTECTION OF OTHER FEDERAL PRIVACY  
12 LAWS.—Nothing in this title may be construed to modify,  
13 limit, or supersede the operation of the Federal privacy  
14 laws described in subsection (d) or the provision of infor-  
15 mation permitted or required, expressly or by implication,  
16 by such laws, with respect to Federal rights and practices.

17 (c) COMMUNICATIONS INFRASTRUCTURE AND PRI-  
18 VACY.—If a person is subject to a provision of section 222  
19 or 631 of the Communications Act of 1934 (47 U.S.C.  
20 222 and 551) and a provision of this title, such provision  
21 of such section 222 or 631 shall not apply to such person  
22 to the extent that such provision of this title applies to  
23 such person.

1 (d) OTHER FEDERAL PRIVACY LAWS DESCRIBED.—

2 The Federal privacy laws described in this subsection are  
3 as follows:

4 (1) Section 552a of title 5, United States Code  
5 (commonly known as the Privacy Act of 1974).

6 (2) The Right to Financial Privacy Act of 1978  
7 (12 U.S.C. 3401 et seq.).

8 (3) The Fair Credit Reporting Act (15 U.S.C.  
9 1681 et seq.).

10 (4) The Fair Debt Collection Practices Act (15  
11 U.S.C. 1692 et seq.).

12 (5) The Children’s Online Privacy Protection  
13 Act of 1998 (15 U.S.C. 6501 et seq.).

14 (6) Title V of the Gramm-Leach-Bliley Act of  
15 1999 (15 U.S.C. 6801 et seq.).

16 (7) Chapters 119, 123, and 206 of title 18,  
17 United States Code.

18 (8) Section 2710 of title 18, United States  
19 Code.

20 (9) Section 444 of the General Education Pro-  
21 visions Act (20 U.S.C. 1232g) (commonly referred  
22 to as the “Family Educational Rights and Privacy  
23 Act of 1974”).

24 (10) Section 445 of the General Education Pro-  
25 visions Act (20 U.S.C. 1232h).

1           (11) The Privacy Protection Act of 1980 (42  
2       U.S.C. 2000aa et seq.).

3           (12) The regulations promulgated under section  
4       264(c) of the Health Insurance Portability and Ac-  
5       countability Act of 1996 (42 U.S.C. 1320d–2 note),  
6       as such regulations relate to a person described in  
7       section 1172(a) of the Social Security Act (42  
8       U.S.C. 1320d–1(a)) or to transactions referred to in  
9       section 1173(a)(1) of such Act (42 U.S.C. 1320d–  
10      2(a)(1)).

11          (13) The Communications Assistance for Law  
12      Enforcement Act (47 U.S.C. 1001 et seq.).

13          (14) Section 227 of the Communications Act of  
14      1934 (47 U.S.C. 227).

15      **Subtitle H—Development of Com-**  
16      **mercial Data Privacy Policy in**  
17      **the Department of Commerce**

18      **SEC. 181. DIRECTION TO DEVELOP COMMERCIAL DATA PRI-**  
19      **VACY POLICY.**

20      The Secretary of Commerce shall contribute to the  
21      development of commercial data privacy policy by—

22          (1) convening private sector stakeholders, in-  
23      cluding members of industry, civil society groups,  
24      academia, in open forums, to develop codes of con-

1 duct in support of applications for safe harbor pro-  
2 grams under subtitle F;

3 (2) expanding interoperability between the  
4 United States commercial data privacy framework  
5 and other national and regional privacy frameworks;

6 (3) conducting research related to improving  
7 privacy protection under this title; and

8 (4) conducting research related to improving  
9 data sharing practices, including the use of  
10 anonymised data, and growing the information econ-  
11 omy.

## 12 **TITLE II—ONLINE PRIVACY OF** 13 **CHILDREN**

### 14 **SEC. 201. SHORT TITLE.**

15 This title may be cited as the “Do Not Track Kids  
16 Act of 2017”.

### 17 **SEC. 202. FINDINGS.**

18 Congress finds the following:

19 (1) Since the enactment of the Children’s On-  
20 line Privacy Protection Act of 1998, the World Wide  
21 Web has changed dramatically, with the creation of  
22 tens of millions of websites, the proliferation of en-  
23 tirely new media platforms, and the emergence of a  
24 diverse ecosystem of services, devices, and applica-  
25 tions that enable users to connect wirelessly within

1 an online environment without being tethered to a  
2 desktop computer.

3 (2) The explosive growth of the Internet eco-  
4 system has unleashed a wide array of opportunities  
5 to learn, communicate, participate in civic life, ac-  
6 cess entertainment, and engage in commerce.

7 (3) In addition to these significant benefits, the  
8 Internet also presents challenges, particularly with  
9 respect to the efforts of entities to track the online  
10 activities of children and minors and to collect, use,  
11 and disclose personal information about them, in-  
12 cluding their geolocation, for commercial purposes.

13 (4) Children and teens are visiting numerous  
14 companies' websites, and marketers are using multi-  
15 media games, online quizzes, and mobile phone and  
16 tablet applications to create ties to children and  
17 teens.

18 (5) According to a study by the Wall Street  
19 Journal in 2010, websites directed to children and  
20 teens were more likely to use cookies and other  
21 tracking tools than sites directed to a general audi-  
22 ence.

23 (6) This study examined 50 popular websites  
24 for children and teens in the United States and  
25 found that these 50 sites placed 4,123 cookies, bea-

1 cons, and other tracking tools on the test computer  
2 used for the study.

3 (7) This is 30-percent greater than the number  
4 of such tracking tools that were placed on the test  
5 computer in a similar study of the 50 overall most  
6 popular websites in the United States, which are  
7 generally directed to adults.

8 (8) Children and teens lack the cognitive ability  
9 to distinguish advertising from program content and  
10 to understand that the purpose of advertising is to  
11 persuade them, making them unable to activate the  
12 defenses on which adults rely.

13 (9) Children and teens are less able than adults  
14 to understand the potential long-term consequences  
15 of having their information available to third parties,  
16 including advertisers, and other individuals.

17 (10) According to Common Sense Media and  
18 the Center for Digital Democracy, 90 percent of  
19 teens have used some form of social media, 75 per-  
20 cent have a social networking site, and 51 percent  
21 check their social networking site at least once a  
22 day.

23 (11) Ninety-one percent of parents and 91 per-  
24 cent of adults believe it is not okay for advertisers

1 to collect information about a child's location from  
2 that child's mobile phone.

3 (12) Ninety-four percent of parents and 91 per-  
4 cent of adults agree that advertisers should receive  
5 the parent's permission before putting tracking soft-  
6 ware on a child's computer.

7 (13) Ninety-six percent of parents and 94 per-  
8 cent of adults expressed disapproval when asked if  
9 it is "okay for a website to ask children for personal  
10 information about their friends".

11 (14) Eighty-eight percent of parents would sup-  
12 port a law that requires search engines and social  
13 networking sites to get users' permission before  
14 using their personal information.

15 (15) A Commonsense Media/Zogby poll found  
16 that 94 percent of parents and 94 percent of adults  
17 believe individuals should have the ability to request  
18 the deletion, after a specific period of time, of all of  
19 their personal information held by an online search  
20 engine, social networking site, or marketing com-  
21 pany.

22 (16) According to a Pew/Berkman Center poll,  
23 69 percent of parents of teens who engage in online  
24 activity are concerned about how that activity might

1       affect their children’s future academic or employ-  
 2       ment opportunities.

3               (17) Eighty-one percent of parents of teens who  
 4       engage in online activity say they are concerned  
 5       about how much information advertisers can learn  
 6       about their children’s online activity.

7   **SEC. 203. DEFINITIONS.**

8       (a) IN GENERAL.—In this title:

9               (1) MINOR.—The term “minor” means an indi-  
 10      vidual who is older than 12 years of age and young-  
 11      er than 16 years of age.

12              (2) TARGETED MARKETING.—The term “tar-  
 13      geted marketing” means advertising or other efforts  
 14      to market a product or service that are directed to  
 15      a specific individual or device—

16                      (A) based on the personal information of  
 17                      the individual or a unique identifier of the de-  
 18                      vice; and

19                      (B) as a result of use by the individual, or  
 20                      access by the device, of a website, online serv-  
 21                      ice, online application, or mobile application.

22      (b) TERMS DEFINED BY COMMISSION.—In this title,  
 23      the terms “directed to minors” and “geolocation informa-  
 24      tion” shall have the meanings given such terms by the  
 25      Commission by regulation. Not later than 1 year after the

1 date of enactment of this Act, the Commission shall pro-  
 2 mulgate, under section 553 of title 5, United States Code,  
 3 regulations that define such terms broadly enough so that  
 4 they are not limited to current technology, consistent with  
 5 the principles articulated by the Commission regarding the  
 6 definition of the term “Internet” in its statement of basis  
 7 and purpose on the final rule under the Children’s Online  
 8 Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.)  
 9 promulgated on November 3, 1999 (64 Fed. Reg. 59891).

10 (c) OTHER DEFINITIONS.—The definitions set forth  
 11 in section 1302 of the Children’s Online Privacy Protec-  
 12 tion Act of 1998 (15 U.S.C. 6501), as amended by section  
 13 3(a), shall apply in this title, except to the extent the Com-  
 14 mission provides otherwise by regulations issued under  
 15 section 553 of title 5, United States Code.

16 **SEC. 204. ONLINE COLLECTION, USE, AND DISCLOSURE OF**  
 17 **PERSONAL INFORMATION OF CHILDREN.**

18 (a) DEFINITIONS.—Section 1302 of the Children’s  
 19 Online Privacy Protection Act of 1998 (15 U.S.C. 6501)  
 20 is amended—

21 (1) by amending paragraph (2) to read as fol-  
 22 lows:

23 “(2) OPERATOR.—The term ‘operator’—

24 “(A) means any person who, for commer-  
 25 cial purposes, in interstate or foreign commerce,

operates or provides a website on the Internet,  
online service, online application, or mobile ap-  
plication, and who—

“(i) collects or maintains, either di-  
rectly or through a service provider, per-  
sonal information from or about the users  
of such website, service, or application;

“(ii) allows another person to collect  
personal information directly from users of  
such website, service, or application (in  
which case the operator is deemed to have  
collected the information); or

“(iii) allows users of such website,  
service, or application to publicly disclose  
personal information (in which case the op-  
erator is deemed to have collected the in-  
formation); and

“(B) does not include any nonprofit entity  
that would otherwise be exempt from coverage  
under section 5 of the Federal Trade Commis-  
sion Act (15 U.S.C. 45).”;

(2) in paragraph (4)—

(A) by amending subparagraph (A) to read  
as follows:

1           “(A) the release of personal information  
2           for any purpose, except where such information  
3           is provided to a person other than an operator  
4           who provides support for the internal operations  
5           of the website, online service, online application,  
6           or mobile application of the operator and does  
7           not disclose or use that information for any  
8           other purpose; and”;

9           (B) in subparagraph (B), by striking  
10          “website or online service” and inserting  
11          “website, online service, online application, or  
12          mobile application”;

13         (3) in paragraph (8)—

14                 (A) by amending subparagraph (G) to read  
15                 as follows:

16                         “(G) information concerning a child or the  
17                         parents of that child (including any unique or  
18                         substantially unique identifier, such as a cus-  
19                         tomer number) that an operator collects online  
20                         from the child and combines with an identifier  
21                         described in subparagraphs (A) through (G).”;

22                         (B) by redesignating subparagraphs (F)  
23                         and (G) as subparagraphs (G) and (H), respec-  
24                         tively; and

1 (C) by inserting after subparagraph (E)  
 2 the following new subparagraph:

3 “(F) information (including an Internet  
 4 protocol address) that permits the identification  
 5 of an individual, the computer of an individual,  
 6 or any other device used by an individual to ac-  
 7 cess the Internet or an online service, online ap-  
 8 plication, or mobile application;”;

9 (4) by striking paragraph (10) and redesign-  
 10 ating paragraphs (11) and (12) as paragraphs (10)  
 11 and (11), respectively; and

12 (5) by adding at the end the following new  
 13 paragraph:

14 “(12) ONLINE, ONLINE SERVICE, ONLINE AP-  
 15 PPLICATION, MOBILE APPLICATION, DIRECTED TO  
 16 CHILDREN.—The terms ‘online’, ‘online service’, ‘on-  
 17 line application’, ‘mobile application’, and ‘directed  
 18 to children’ shall have the meanings given such  
 19 terms by the Commission by regulation. Not later  
 20 than 1 year after the date of enactment of the Com-  
 21 mercial Privacy Bill of Rights Act of 2017, the Com-  
 22 mission shall promulgate, under section 553 of title  
 23 5, United States Code, regulations that define such  
 24 terms broadly enough so that they are not limited to  
 25 current technology, consistent with the principles ar-

1        ticated by the Commission regarding the definition  
 2        of the term ‘Internet’ in its statement of basis and  
 3        purpose on the final rule under this title promul-  
 4        gated on November 3, 1999 (64 Fed. Reg. 59891).  
 5        The definition of the term ‘online service’ in such  
 6        regulations shall include broadband Internet access  
 7        service (as defined in the Report and Order of the  
 8        Federal Communications Commission relating to the  
 9        matter of preserving the open Internet and  
 10        broadband industry practices (FCC 10–201, adopted  
 11        by the Commission on December 21, 2010)).”.

12        (b) **ONLINE COLLECTION, USE, AND DISCLOSURE OF**  
 13 **PERSONAL INFORMATION OF CHILDREN.**—Section 1303  
 14 of the Children’s Online Privacy Protection Act of 1998  
 15 (15 U.S.C. 6502) is amended—

16            (1) by striking the heading and inserting the  
 17        following: “**ONLINE COLLECTION, USE, AND DIS-**  
 18        **CLOSURE OF PERSONAL INFORMATION OF**  
 19        **CHILDREN.**”;

20            (2) in subsection (a)—

21            (A) by amending paragraph (1) to read as  
 22        follows:

23            “(1) **IN GENERAL.**—It is unlawful for an oper-  
 24        ator of a website, online service, online application,  
 25        or mobile application directed to children, or an op-

erator having actual knowledge that personal information being collected is from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b).”; and

(B) in paragraph (2)—

(i) by striking “of such a website or online service”; and

(ii) by striking “subsection (b)(1)(B)(iii)” and inserting “subsection (b)(1)(C)(iii)”; and

(3) in subsection (b)—

(A) by amending paragraph (1) to read as follows:

“(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Commercial Privacy Bill of Rights Act of 2017, the Commission shall promulgate, under section 553 of title 5, United States Code, regulations to require an operator of a website, online service, online application, or mobile application directed to children, or an operator having actual knowledge that personal information being collected is from a child—

“(A) to provide clear and conspicuous notice in clear and plain language of the types of

1 personal information the operator collects, how  
2 the operator uses such information, whether the  
3 operator discloses such information, and the  
4 procedures or mechanisms the operator uses to  
5 ensure that personal information is not col-  
6 lected from children except in accordance with  
7 the regulations promulgated under this para-  
8 graph;

9 “(B) to obtain verifiable parental consent  
10 for the collection, use, or disclosure of personal  
11 information of a child;

12 “(C) to provide to a parent whose child  
13 has provided personal information to the oper-  
14 ator, upon request by and proper identification  
15 of the parent—

16 “(i) a description of the specific types  
17 of personal information collected from the  
18 child by the operator;

19 “(ii) the opportunity at any time to  
20 refuse to permit the further use or mainte-  
21 nance in retrievable form, or future collec-  
22 tion, by the operator of personal informa-  
23 tion collected from the child; and

24 “(iii) a means that is reasonable  
25 under the circumstances for the parent to

1           obtain any personal information collected  
 2           from the child, if such information is avail-  
 3           able to the operator at the time the parent  
 4           makes the request;

5           “(D) not to condition participation in a  
 6           game, or use of a website, service, or applica-  
 7           tion, by a child on the provision by the child of  
 8           more personal information than is reasonably  
 9           required to participate in the game or use the  
 10          website, service, or application; and

11          “(E) to establish and maintain reasonable  
 12          procedures to protect the confidentiality, secu-  
 13          rity, and integrity of personal information col-  
 14          lected from children.”;

15          (B) in paragraph (2)—

16               (i) in the matter preceding subpara-  
 17               graph (A), by striking “paragraph  
 18               (1)(A)(ii)” and inserting “paragraph  
 19               (1)(B)”;

20               (ii) in subparagraph (A), by inserting  
 21               “or to contact a different child” after “to  
 22               recontact the child”;

23          (C) by amending paragraph (3) to read as  
 24          follows:

1           “(3) CONTINUATION OF SERVICE.—The regula-  
 2           tions shall prohibit an operator from discontinuing  
 3           service provided to a child on the basis of refusal by  
 4           the parent of the child, under the regulations pre-  
 5           scribed under paragraph (1)(C)(ii), to permit the  
 6           further use or maintenance in retrievable form, or  
 7           future collection, by the operator of personal infor-  
 8           mation collected from the child, to the extent that  
 9           the operator is capable of providing such service  
 10          without such information.”; and

11                         (D) by adding at the end the following:

12           “(4) RULE FOR TREATMENT OF USERS OF  
 13           WEBSITES, SERVICES, AND APPLICATIONS DIRECTED  
 14           TO CHILDREN.—An operator of a website, online  
 15           service, online application, or mobile application that  
 16           is directed to children shall treat all users of such  
 17           website, service, or application as children for pur-  
 18           poses of this title, except as permitted by the Com-  
 19           mission by a regulation promulgated under this  
 20           title.”.

21           (c) ADMINISTRATION AND APPLICABILITY OF ACT.—  
 22           Section 1306 of the Children’s Online Privacy Protection  
 23           Act of 1998 (15 U.S.C. 6505) is amended—

24                         (1) in subsection (b)—

1 (A) in paragraph (1), by striking “, in the  
 2 case of” and all that follows and inserting the  
 3 following: “by the appropriate Federal banking  
 4 agency with respect to any insured depository  
 5 institution (as such terms are defined in section  
 6 3 of such Act (12 U.S.C. 1813));”; and

7 (B) by striking paragraph (2) and redesign-  
 8 ating paragraphs (3) through (6) as para-  
 9 graphs (2) through (5), respectively; and

10 (2) by adding at the end the following new sub-  
 11 section:

12 “(f) TELECOMMUNICATIONS CARRIERS AND CABLE  
 13 OPERATORS.—

14 “(1) ENFORCEMENT BY FTC.—Notwithstanding  
 15 section 5(a)(2) of the Federal Trade Commission  
 16 Act (15 U.S.C. 45(a)(2)), compliance with the re-  
 17 quirements imposed under this title shall be enforced  
 18 by the Commission with respect to any telecommuni-  
 19 cations carrier (as defined in section 3 of the Com-  
 20 munications Act of 1934 (47 U.S.C. 153)).

21 “(2) RELATIONSHIP TO OTHER LAW.—To the  
 22 extent that sections 222, 338(i), and 631 of the  
 23 Communications Act of 1934 (47 U.S.C. 222;  
 24 338(i); 551) are inconsistent with this title, this title  
 25 controls.”.

1 **SEC. 205. TARGETED MARKETING TO CHILDREN OR MI-**  
2 **NORS.**

3 (a) ACTS PROHIBITED.—It is unlawful for—

4 (1) an operator of a website, online service, on-  
5 line application, or mobile application directed to  
6 children, or an operator having actual knowledge  
7 that personal information being collected is from a  
8 child, to use, disclose to third parties, or compile  
9 personal information for targeted marketing pur-  
10 poses without verifiable parental consent; or

11 (2) an operator of a website, online service, on-  
12 line application, or mobile application directed to mi-  
13 nors, or an operator having actual knowledge that  
14 personal information being collected is from a minor,  
15 to use, disclose to third parties, or compile personal  
16 information for targeted marketing purposes without  
17 the consent of the minor.

18 (b) REGULATIONS.—Not later than 1 year after the  
19 date of enactment of this Act, the Commission shall pro-  
20 mulgate, under section 553 of title 5, United States Code,  
21 regulations to implement this section.

22 **SEC. 206. DIGITAL MARKETING BILL OF RIGHTS FOR TEENS**  
23 **AND FAIR INFORMATION PRACTICES PRIN-**  
24 **CIPLES.**

25 (a) ACTS PROHIBITED.—It is unlawful for an oper-  
26 ator of a website, online service, online application, or mo-

1   bile application directed to minors, or an operator having  
 2   actual knowledge that personal information being collected  
 3   is from a minor, to collect personal information from a  
 4   minor unless such operator has adopted and complies with  
 5   a Digital Marketing Bill of Rights for Teens that is con-  
 6   sistent with the Fair Information Practices Principles de-  
 7   scribed in subsection (b).

8       (b) FAIR INFORMATION PRACTICES PRINCIPLES.—  
 9   The Fair Information Practices Principles described in  
 10 this subsection are the following:

11           (1) COLLECTION LIMITATION PRINCIPLE.—Ex-  
 12       cept as provided in paragraph (3), personal informa-  
 13       tion should be collected from a minor only when col-  
 14       lection of the personal information is—

15               (A) consistent with the context of a par-  
 16               ticular transaction or service or the relationship  
 17               of the minor with the operator, including collec-  
 18               tion necessary to fulfill a transaction or provide  
 19               a service requested by the minor; or

20               (B) required or specifically authorized by  
 21       law.

22           (2) DATA QUALITY PRINCIPLE.—The personal  
 23       information of a minor should be accurate, complete,  
 24       and kept up-to-date to the extent necessary to fulfill

1 the purposes described in subparagraphs (A)  
2 through (D) of paragraph (3).

3 (3) PURPOSE SPECIFICATION PRINCIPLE.—The  
4 purposes for which personal information is collected  
5 should be specified to the minor not later than at  
6 the time of the collection of the information. The  
7 subsequent use or disclosure of the information  
8 should be limited to—

9 (A) fulfillment of the transaction or service  
10 requested by the minor;

11 (B) support for the internal operations of  
12 the website, service, or application, as described  
13 in section 312.2 of title 16, Code of Federal  
14 Regulations;

15 (C) compliance with legal process or other  
16 purposes expressly authorized under specific  
17 legal authority; or

18 (D) other purposes—

19 (i) that are specified in a notice to the  
20 minor; and

21 (ii) to which the minor has consented  
22 under paragraph (7) before the informa-  
23 tion is used or disclosed for such other  
24 purposes.

1           (4) RETENTION LIMITATION PRINCIPLE.—The  
2       personal information of a minor should not be re-  
3       tained for longer than is necessary to fulfill a trans-  
4       action or provide a service requested by the minor  
5       or such other purposes specified in subparagraphs  
6       (A) through (D) of paragraph (3). The operator  
7       should implement a reasonable and appropriate data  
8       disposal policy based on the nature and sensitivity of  
9       such personal information.

10          (5) SECURITY SAFEGUARDS PRINCIPLE.—The  
11       personal information of a minor should be protected  
12       by reasonable and appropriate security safeguards  
13       against risks such as loss or unauthorized access,  
14       destruction, use, modification, or disclosure.

15          (6) OPENNESS PRINCIPLE.—

16                (A) IN GENERAL.—The operator should  
17       maintain a general policy of openness about de-  
18       velopments, practices, and policies with respect  
19       to the personal information of a minor. The op-  
20       erator should provide each minor using the  
21       website, online service, online application, or  
22       mobile application of the operator with a clear  
23       and prominent means—

24                   (i) to identify and contact the oper-  
25       ator, by, at a minimum, disclosing, clearly

1 and prominently, the identity of the oper-  
2 ator and—

3 (I) in the case of an operator  
4 who is an individual, the address of  
5 the principal residence of the operator  
6 and an e-mail address and telephone  
7 number for the operator; or

8 (II) in the case of any other op-  
9 erator, the address of the principal  
10 place of business of the operator and  
11 an e-mail address and telephone num-  
12 ber for the operator;

13 (ii) to determine whether the operator  
14 possesses any personal information of the  
15 minor, the nature of any such information,  
16 and the purposes for which the information  
17 was collected and is being retained;

18 (iii) to obtain any personal informa-  
19 tion of the minor that is in the possession  
20 of the operator from the operator, or from  
21 a person specified by the operator, within  
22 a reasonable time after making a request,  
23 at a charge (if any) that is not excessive,  
24 in a reasonable manner, and in a form that  
25 is readily intelligible to the minor;

1 (iv) to challenge the accuracy of per-  
 2 sonal information of the minor that is in  
 3 the possession of the operator; and

4 (v) if the minor establishes the inaccu-  
 5 racy of personal information in a challenge  
 6 under clause (iv), to have such information  
 7 erased, corrected, completed, or otherwise  
 8 amended.

9 (B) LIMITATION.—Nothing in this para-  
 10 graph shall be construed to permit an operator  
 11 to erase or otherwise modify personal informa-  
 12 tion requested by a law enforcement agency  
 13 pursuant to legal authority.

14 (7) INDIVIDUAL PARTICIPATION PRINCIPLE.—  
 15 The operator should—

16 (A) obtain consent from a minor before  
 17 using or disclosing the personal information of  
 18 the minor for any purpose other than the pur-  
 19 poses described in subparagraphs (A) through  
 20 (C) of paragraph (3); and

21 (B) obtain affirmative express consent  
 22 from a minor before using or disclosing pre-  
 23 viously collected personal information of the  
 24 minor for purposes that constitute a material

1 change in practice from the original purposes  
 2 specified to the minor under paragraph (3).

3 (c) REGULATIONS.—Not later than 1 year after the  
 4 date of enactment of this Act, the Commission shall pro-  
 5 mulgate, under section 553 of title 5, United States Code,  
 6 regulations to implement this section, including regula-  
 7 tions further defining the Fair Information Practices  
 8 Principles described in subsection (b).

9 **SEC. 207. ONLINE COLLECTION OF GEOLOCATION INFOR-**  
 10 **MATION OF CHILDREN AND MINORS.**

11 (a) ACTS PROHIBITED.—

12 (1) IN GENERAL.—It is unlawful for an oper-  
 13 ator of a website, online service, online application,  
 14 or mobile application directed to children or minors,  
 15 or an operator having actual knowledge that  
 16 geolocation information being collected is from a  
 17 child or minor, to collect geolocation information  
 18 from a child or minor in a manner that violates the  
 19 regulations prescribed under subsection (b).

20 (2) DISCLOSURE TO PARENT OR MINOR PRO-  
 21 TECTED.—Notwithstanding paragraph (1), neither  
 22 an operator nor the operator's agent shall be held to  
 23 be liable under any Federal or State law for any dis-  
 24 closure made in good faith and following reasonable  
 25 procedures in responding to a request for disclosure

1 of geolocation information under subparagraph  
2 (C)(ii)(III) or (D)(ii)(III) of subsection (b)(1).

3 (b) REGULATIONS.—

4 (1) IN GENERAL.—Not later than 1 year after  
5 the date of enactment of this Act, the Commission  
6 shall promulgate, under section 553 of title 5,  
7 United States Code, regulations that require an op-  
8 erator of a website, online service, online application,  
9 or mobile application directed to children or minors,  
10 or an operator having actual knowledge that  
11 geolocation information being collected is from a  
12 child or minor—

13 (A) to provide clear and conspicuous notice  
14 in clear and plain language of any geolocation  
15 information the operator collects, how the oper-  
16 ator uses such information, and whether the op-  
17 erator discloses such information;

18 (B) to establish procedures or mechanisms  
19 to ensure that geolocation information is not  
20 collected from children or minors except in ac-  
21 cordance with regulations promulgated under  
22 this paragraph;

23 (C) in the case of collection of geolocation  
24 information from a child—

1 (i) prior to collecting such informa-  
2 tion, to obtain verifiable parental consent;  
3 and

4 (ii) after collecting such information,  
5 to provide to the parent of the child, upon  
6 request by and proper identification of the  
7 parent—

8 (I) a description of the  
9 geolocation information collected from  
10 the child by the operator;

11 (II) the opportunity at any time  
12 to refuse to permit the further use or  
13 maintenance in retrievable form, or  
14 future collection, by the operator of  
15 geolocation information from the  
16 child; and

17 (III) a means that is reasonable  
18 under the circumstances for the par-  
19 ent to obtain any geolocation informa-  
20 tion collected from the child, if such  
21 information is available to the oper-  
22 ator at the time the parent makes the  
23 request; and

24 (D) in the case of collection of geolocation  
25 information from a minor—

1 (i) prior to collecting such informa-  
 2 tion, to obtain affirmative express consent  
 3 from such minor; and

4 (ii) after collecting such information,  
 5 to provide to the minor, upon request—

6 (I) a description of the  
 7 geolocation information collected from  
 8 the minor by the operator;

9 (II) the opportunity at any time  
 10 to refuse to permit the further use or  
 11 maintenance in retrievable form, or  
 12 future collection, by the operator of  
 13 geolocation information from the  
 14 minor; and

15 (III) a means that is reasonable  
 16 under the circumstances for the minor  
 17 to obtain any geolocation information  
 18 collected from the minor, if such in-  
 19 formation is available to the operator  
 20 at the time the minor makes the re-  
 21 quest.

22 (2) WHEN CONSENT NOT REQUIRED.—The reg-  
 23 ulations promulgated under paragraph (1) shall pro-  
 24 vide that verifiable parental consent under subpara-  
 25 graph (C)(i) of such paragraph or affirmative ex-

1 press consent under subparagraph (D)(i) of such  
2 paragraph is not required when the collection of the  
3 geolocation information of a child or minor is nec-  
4 essary, to the extent permitted under other provi-  
5 sions of law, to provide information to law enforce-  
6 ment agencies or for an investigation on a matter re-  
7 lated to public safety.

8 (3) CONTINUATION OF SERVICE.—The regula-  
9 tions promulgated under paragraph (1) shall pro-  
10 hibit an operator from discontinuing service provided  
11 to—

12 (A) a child on the basis of refusal by the  
13 parent of the child, under subparagraph  
14 (C)(ii)(II) of such paragraph, to permit the fur-  
15 ther use or maintenance in retrievable form, or  
16 future online collection, of geolocation informa-  
17 tion from the child by the operator, to the ex-  
18 tent that the operator is capable of providing  
19 such service without such information; or

20 (B) a minor on the basis of refusal by the  
21 minor, under subparagraph (D)(ii)(II) of such  
22 paragraph, to permit the further use or mainte-  
23 nance in retrievable form, or future online col-  
24 lection, of geolocation information from the  
25 minor by the operator, to the extent that the

1 operator is capable of providing such service  
2 without such information.

3 (c) INCONSISTENT STATE LAW.—No State or local  
4 government may impose any liability for commercial ac-  
5 tivities or actions by operators in interstate or foreign  
6 commerce in connection with an activity or action de-  
7 scribed in this section that is inconsistent with the treat-  
8 ment of those activities or actions under this section.

9 **SEC. 208. REMOVAL OF CONTENT.**

10 (a) ACTS PROHIBITED.—It is unlawful for an oper-  
11 ator of a website, online service, online application, or mo-  
12 bile application to make publicly available through the  
13 website, service, or application content or information that  
14 contains or displays personal information of children or  
15 minors in a manner that violates the regulations pre-  
16 scribed under subsection (b).

17 (b) REGULATIONS.—

18 (1) IN GENERAL.—Not later than 1 year after  
19 the date of enactment of this Act, the Commission  
20 shall promulgate, under section 553 of title 5,  
21 United States Code, regulations that require an op-  
22 erator—

23 (A) to the extent technologically feasible,  
24 to implement mechanisms that permit a user of  
25 the website, service, or application of the oper-

1 ator to erase or otherwise eliminate content or  
2 information submitted to the website, service, or  
3 application by such user that is publicly avail-  
4 able through the website, service, or application  
5 and contains or displays personal information of  
6 children or minors; and

7 (B) to take appropriate steps to make  
8 users aware of such mechanisms and to provide  
9 notice to users that such mechanisms do not  
10 necessarily provide comprehensive removal of  
11 the content or information submitted by such  
12 users.

13 (2) EXCEPTION.—The regulations promulgated  
14 under paragraph (1) may not require an operator or  
15 third party to erase or otherwise eliminate content  
16 or information that—

17 (A) any other provision of Federal or State  
18 law requires the operator or third party to  
19 maintain; or

20 (B) was submitted to the website, service,  
21 or application of the operator by any person  
22 other than the user who is attempting to erase  
23 or otherwise eliminate such content or informa-  
24 tion, including content or information submitted

1           by such user that was republished or resub-  
2           mitted by another person.

3           (3) LIMITATION.—Nothing in this section shall  
4           be construed to limit the authority of a law enforce-  
5           ment agency to obtain any content or information  
6           from an operator as authorized by law or pursuant  
7           to an order of a court of competent jurisdiction.

8   **SEC. 209. ENFORCEMENT AND APPLICABILITY.**

9           (a) ENFORCEMENT BY THE COMMISSION.—

10           (1) IN GENERAL.—Except as otherwise pro-  
11           vided, this title and the regulations prescribed under  
12           this title shall be enforced by the Commission under  
13           the Federal Trade Commission Act (15 U.S.C. 41 et  
14           seq.).

15           (2) UNFAIR OR DECEPTIVE ACTS OR PRAC-  
16           TICES.—Subject to subsection (b), a violation of this  
17           title or a regulation prescribed under this title shall  
18           be treated as a violation of a rule defining an unfair  
19           or deceptive act or practice prescribed under section  
20           18(a)(1)(B) of the Federal Trade Commission Act  
21           (15 U.S.C. 57a(a)(1)(B)).

22           (3) ACTIONS BY THE COMMISSION.—

23           (A) IN GENERAL.—Subject to subsection  
24           (b), and except as provided in subsection (d)(1),  
25           the Commission shall prevent any person from

1           violating this title or a regulation prescribed  
 2           under this title in the same manner, by the  
 3           same means, and with the same jurisdiction,  
 4           powers, and duties as though all applicable  
 5           terms and provisions of the Federal Trade  
 6           Commission Act (15 U.S.C. 41 et seq.) were in-  
 7           corporated into and made a part of this title.

8                   (B) PRIVILEGES AND IMMUNITIES.—Any  
 9           person who violates this title or a regulation  
 10          prescribed under this title shall be subject to  
 11          the penalties and entitled to the privileges and  
 12          immunities provided in the Federal Trade Com-  
 13          mission Act (15 U.S.C. 41 et seq.).

14          (b) ENFORCEMENT BY CERTAIN OTHER AGEN-  
 15          CIES.—Notwithstanding subsection (a), compliance with  
 16          the requirements imposed under this title shall be enforced  
 17          as follows:

18                (1) Under section 8 of the Federal Deposit In-  
 19          surance Act (12 U.S.C. 1818) by the appropriate  
 20          Federal banking agency, with respect to an insured  
 21          depository institution (as such terms are defined in  
 22          section 3 of such Act (12 U.S.C. 1813)).

23                (2) Under the Federal Credit Union Act (12  
 24          U.S.C. 1751 et seq.) by the National Credit Union

1 Administration Board, with respect to any Federal  
2 credit union.

3 (3) Under part A of subtitle VII of title 49,  
4 United States Code, by the Secretary of Transpor-  
5 tation, with respect to any air carrier or foreign air  
6 carrier subject to such part.

7 (4) Under the Packers and Stockyards Act,  
8 1921 (7 U.S.C. 181 et seq.) (except as provided in  
9 section 406 of such Act (7 U.S.C. 226; 227)) by the  
10 Secretary of Agriculture, with respect to any activi-  
11 ties subject to such Act.

12 (5) Under the Farm Credit Act of 1971 (12  
13 U.S.C. 2001 et seq.) by the Farm Credit Adminis-  
14 tration, with respect to any Federal land bank, Fed-  
15 eral land bank association, Federal intermediate  
16 credit bank, or production credit association.

17 (c) ENFORCEMENT BY STATES.—

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

1 court of the United States of appropriate jurisdic-  
 2 tion to—

3 (A) enjoin that practice;

4 (B) enforce compliance with this title or  
 5 such regulation;

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

9 (D) obtain such other relief as the court  
 10 may consider to be appropriate.

11 (2) RIGHTS OF FEDERAL TRADE COMMIS-  
 12 SION.—

13 (A) NOTICE TO FEDERAL TRADE COMMIS-  
 14 SION.—

15 (i) IN GENERAL.—Except as provided  
 16 in clause (iii), the attorney general of a  
 17 State shall notify the Federal Trade Com-  
 18 mission in writing that the attorney gen-  
 19 eral intends to bring a civil action under  
 20 paragraph (1) before initiating the civil ac-  
 21 tion.

22 (ii) CONTENTS.—The notification re-  
 23 quired by clause (i) with respect to a civil  
 24 action shall include a copy of the complaint  
 25 to be filed to initiate the civil action.

1 (iii) EXCEPTION.—If it is not feasible  
 2 for the attorney general of a State to pro-  
 3 vide the notification required by clause (i)  
 4 before initiating a civil action under para-  
 5 graph (1), the attorney general shall notify  
 6 the Federal Trade Commission imme-  
 7 diately upon instituting the civil action.

8 (B) INTERVENTION BY FEDERAL TRADE  
 9 COMMISSION.—The Federal Trade Commission  
 10 may—

11 (i) intervene in any civil action  
 12 brought by the attorney general of a State  
 13 under paragraph (1); and

14 (ii) upon intervening—

15 (I) be heard on all matters aris-  
 16 ing in the civil action; and

17 (II) file petitions for appeal of a  
 18 decision in the civil action.

19 (3) INVESTIGATORY POWERS.—For purposes of  
 20 bringing any civil action under paragraph (1), noth-  
 21 ing in this title shall be construed to prevent an at-  
 22 torney general of a State from exercising the powers  
 23 conferred on the attorney general by the laws of that  
 24 State to—

25 (A) conduct investigations;

1 (B) administer oaths or affirmations; or

2 (C) compel the attendance of witnesses or  
3 the production of documentary and other evi-  
4 dence.

5 (4) PREEMPTIVE ACTION BY FEDERAL TRADE  
6 COMMISSION.—If the Federal Trade Commission in-  
7 stitutes a civil action or an administrative action  
8 with respect to a violation of this title, the attorney  
9 general of a State may not, during the pendency of  
10 such action, bring a civil action under paragraph (1)  
11 against any defendant named in the complaint of the  
12 Commission for the violation with respect to which  
13 the Commission instituted such action.

14 (5) VENUE; SERVICE OF PROCESS.—

15 (A) VENUE.—Any action brought under  
16 paragraph (1) may be brought in the district  
17 court of the United States that meets applicable  
18 requirements relating to venue under section  
19 1391 of title 28, United States Code.

20 (B) SERVICE OF PROCESS.—In an action  
21 brought under paragraph (1), process may be  
22 served in any district in which the defendant—

23 (i) is an inhabitant; or

24 (ii) may be found.

25 (6) ACTIONS BY OTHER STATE OFFICIALS.—

1 (A) IN GENERAL.—In addition to civil ac-  
 2 tions brought by attorneys general under para-  
 3 graph (1), any other officer of a State who is  
 4 authorized by the State to do so may bring a  
 5 civil action under paragraph (1), subject to the  
 6 same requirements and limitations that apply  
 7 under this subsection to civil actions brought by  
 8 attorneys general.

9 (B) SAVINGS PROVISION.—Nothing in this  
 10 subsection may be construed to prohibit an au-  
 11 thorized official of a State from initiating or  
 12 continuing any proceeding in a court of the  
 13 State for a violation of any civil or criminal law  
 14 of the State.

15 (d) TELECOMMUNICATIONS CARRIERS AND CABLE  
 16 OPERATORS.—

17 (1) ENFORCEMENT BY FTC.—Notwithstanding  
 18 section 5(a)(2) of the Federal Trade Commission  
 19 Act (15 U.S.C. 45(a)(2)), compliance with the re-  
 20 quirements imposed under this title shall be enforced  
 21 by the Commission with respect to any telecommuni-  
 22 cations carrier (as defined in section 3 of the Com-  
 23 munications Act of 1934 (47 U.S.C. 153)).

24 (2) RELATIONSHIP TO OTHER LAW.—To the ex-  
 25 tent that sections 222, 338(i), and 631 of the Com-

1       munications Act of 1934 (47 U.S.C. 222; 338(i);  
2       551) are inconsistent with this title, this title con-  
3       trols.

4   **SEC. 210. RULE FOR TREATMENT OF USERS OF WEBSITES,**  
5                   **SERVICES, AND APPLICATIONS DIRECTED TO**  
6                   **CHILDREN OR MINORS.**

7       An operator of a website, online service, online appli-  
8       cation, or mobile application that is directed to children  
9       or minors shall treat all users of such website, service, or  
10      application as children or minors (as the case may be) for  
11      purposes of this title, except as permitted by the Commis-  
12      sion by a regulation promulgated under this title.

13   **SEC. 211. EFFECTIVE DATES.**

14       (a) IN GENERAL.—Except as provided in subsections  
15      (b) and (c), this title and the amendments made by this  
16      title shall take effect on the date that is 1 year after the  
17      date of enactment of this Act.

18       (b) AUTHORITY TO PROMULGATE REGULATIONS.—  
19      The following shall take effect on the date of enactment  
20      of this Act:

21           (1) The amendments made by subsections  
22      (a)(5) and (b)(3)(A) of section 204.

23           (2) Sections 205(b), 206(c), 207(b), and  
24      208(b).

25           (3) Subsections (b) and (c) of section 203.

1       (c) DIGITAL MARKETING BILL OF RIGHTS FOR  
2 TEENS.—Section 206, except for subsection (c) of such  
3 section, shall take effect on the date that is 180 days after  
4 the promulgation of regulations under such subsection.

