

112TH CONGRESS
1ST SESSION

S. 799

To establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 12, 2011

Mr. KERRY (for himself and Mr. MCCAIN) 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, and for other purposes.

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

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

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Commercial Privacy Bill of Rights Act of 2011”.

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

Sec. 1. Short title; table of contents.

- Sec. 2. Findings.
- Sec. 3. Definitions.

TITLE I—RIGHT TO SECURITY AND ACCOUNTABILITY

- Sec. 101. Security.
- Sec. 102. Accountability.
- Sec. 103. Privacy by design.

TITLE II—RIGHT TO NOTICE AND INDIVIDUAL PARTICIPATION

- Sec. 201. Transparent notice of practices and purposes.
- Sec. 202. Individual participation.

TITLE III—RIGHTS RELATING TO DATA MINIMIZATION, CONSTRAINTS ON DISTRIBUTION, AND DATA INTEGRITY

- Sec. 301. Data minimization.
- Sec. 302. Constraints on distribution of information.
- Sec. 303. Data integrity.

TITLE IV—ENFORCEMENT

- Sec. 401. General application.
- Sec. 402. Enforcement by the Federal Trade Commission.
- Sec. 403. Enforcement by State attorneys general.
- Sec. 404. Civil penalties.
- Sec. 405. Effect on other laws.
- Sec. 406. No private right of action.

TITLE V—CO-REGULATORY SAFE HARBOR PROGRAMS

- Sec. 501. Establishment of safe harbor programs.
- Sec. 502. Participation in safe harbor program.

TITLE VI—APPLICATION WITH OTHER FEDERAL LAWS

- Sec. 601. Application with other Federal laws.

TITLE VII—DEVELOPMENT OF COMMERCIAL DATA PRIVACY POLICY IN THE DEPARTMENT OF COMMERCE

- Sec. 701. Direction to develop commercial data privacy policy.

1 **SEC. 2. FINDINGS.**

2 The Congress finds the following:

3 (1) Personal privacy is worthy of protection
4 through appropriate legislation.

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

1 (3) Persons interacting with others engaged in
2 interstate commerce have a significant interest in
3 their personal information, as well as a right to con-
4 trol how that information is collected, used, stored,
5 or transferred.

6 (4) Persons engaged in interstate commerce
7 and collecting personally identifiable information on
8 individuals have a responsibility to treat that infor-
9 mation with respect and in accordance with common
10 standards.

11 (5) To the extent that States regulate the treat-
12 ment of personally identifiable information, their ef-
13 forts to address Internet privacy could lead to a
14 patchwork of inconsistent standards and protections.

15 (6) On the day before the date of the enactment
16 of this Act, the laws of the Federal Government and
17 State and local governments provided inadequate
18 privacy protection for individuals engaging in and
19 interacting with persons engaged in interstate com-
20 merce.

21 (7) As of the day before the date of the enact-
22 ment of this Act, with the exception of Federal
23 Trade Commission enforcement of laws against un-
24 fair and deceptive practices, the Federal Government
25 has eschewed general commercial privacy laws in

1 favor of industry self-regulation, which has led to
2 several self-policing schemes, some of which are en-
3 forceable, and some of which provide insufficient pri-
4 vacy protection to individuals.

5 (8) As of the day before the date of the enact-
6 ment of this Act, many collectors of personally iden-
7 tifiable information have yet to provide baseline fair
8 information practice protections for individuals.

9 (9) The ease of gathering and compiling per-
10 sonal information on the Internet and off, both
11 overtly and surreptitiously, is becoming increasingly
12 efficient and effortless due to advances in technology
13 which have provided information gatherers the abil-
14 ity to compile seamlessly highly detailed personal
15 histories of individuals.

16 (10) Personal information requires greater pri-
17 vacy protection than is available on the day before
18 the date of the enactment of this Act. Vast amounts
19 of personal information, including sensitive informa-
20 tion, about individuals are collected on and off the
21 Internet, often combined and sold or otherwise
22 transferred to third parties, for purposes unknown
23 to an individual to whom the personally identifiable
24 information pertains.

1 (11) Toward the close of the 20th Century, as
2 individuals' personal information was increasingly
3 collected, profiled, and shared for commercial pur-
4 poses, and as technology advanced to facilitate these
5 practices, Congress enacted numerous statutes to
6 protect privacy.

7 (12) Those statutes apply to the government,
8 telephones, cable television, e-mail, video tape rent-
9 als, and the Internet (but only with respect to chil-
10 dren and law enforcement requests).

11 (13) As in those instances, the Federal Govern-
12 ment has a substantial interest in creating a level
13 playing field of protection across all collectors of per-
14 sonally identifiable information, both in the United
15 States and abroad.

16 (14) The Federal Trade Commission has called
17 private self regulation efforts as of the day before
18 the date of the introduction of this Act inadequate.
19 The Commission has also distinguished publishers'
20 first-party data collection practices from third-party
21 practices related specifically to behavioral adver-
22 tising. The Commission has noted that when dealing
23 directly with an Internet website, consumers are
24 likely to understand why they receive a recommenda-

1 tion or advertisement from that entity and may ex-
2 pect it.

3 (15) 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. 3. DEFINITIONS.**

12 In this Act:

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

15 (2) COVERED ENTITY.—The term “covered en-
16 tity” means any person to whom this Act applies
17 under section 401.

18 (3) COVERED INFORMATION.—

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

22 (i) Personally identifiable information.

23 (ii) Unique identifier information.

24 (iii) Any information that is collected,
25 used, or stored in connection with person-

1 ally identifiable information or unique
2 identifier information in a manner that
3 may reasonably be used by the party col-
4 lecting the information to identify a spe-
5 cific individual.

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

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

12 (ii) Personally identifiable information
13 that is obtained from a forum—

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

18 (II) that—

19 (aa) is widely and publicly
20 available; and

21 (bb) contains no restrictions
22 on who can access and view such
23 information.

24 (iii) Personally identifiable informa-
25 tion reported in public media.

1 (iv) Personally identifiable informa-
2 tion dedicated to contacting an individual
3 at the individual's place of work.

4 (4) ESTABLISHED BUSINESS RELATIONSHIP.—
5 The term “established business relationship” means,
6 with respect to a covered entity and a person, a rela-
7 tionship formed with or without the exchange of con-
8 sideration, involving the establishment of an account
9 by the person with the covered entity for the receipt
10 of products or services offered by the covered entity.

11 (5) PERSONALLY IDENTIFIABLE INFORMA-
12 TION.—The term “personally identifiable informa-
13 tion” means only the following:

14 (A) Any of the following information about
15 an individual:

16 (i) The first name (or initial) and last
17 name of an individual, whether given at
18 birth or time of adoption, or resulting from
19 a lawful change of name.

20 (ii) The postal address of a physical
21 place of residence of such individual.

22 (iii) An e-mail address.

23 (iv) A telephone number or mobile de-
24 vice number.

1 (v) A social security number or other
2 government issued identification number
3 issued to such individual.

4 (vi) The account number of a credit
5 card issued to such individual.

6 (vii) Unique identifier information
7 that alone can be used to identify a spe-
8 cific individual.

9 (viii) Biometric data about such indi-
10 vidual, including fingerprints and retina
11 scans.

12 (B) If used, transferred, or stored in con-
13 nection with 1 or more of the items of informa-
14 tion described in subparagraph (A), any of the
15 following:

16 (i) A date of birth.

17 (ii) The number of a certificate of
18 birth or adoption.

19 (iii) A place of birth.

20 (iv) Unique identifier information that
21 alone cannot be used to identify a specific
22 individual.

23 (v) Precise geographic location, at the
24 same degree of specificity as a global posi-
25 tioning system or equivalent system, and

1 not including any general geographic infor-
2 mation that may be derived from an Inter-
3 net Protocol address.

4 (vi) Information about an individual's
5 quantity, technical configuration, type, des-
6 tination, location, and amount of uses of
7 voice services, regardless of technology
8 used.

9 (vii) Any other information concerning
10 an individual that may reasonably be used
11 by the party using, collecting, or storing
12 that information to identify that individual.

13 (6) SENSITIVE PERSONALLY IDENTIFIABLE IN-
14 FORMATION.—The term “sensitive personally identi-
15 fiable information” means—

16 (A) personally identifiable information
17 which, if lost, compromised, or disclosed with-
18 out authorization either alone or with other in-
19 formation, carries a significant risk of economic
20 or physical harm; or

21 (B) information related to—

22 (i) a particular medical condition or a
23 health record; or

24 (ii) the religious affiliation of an indi-
25 vidual.

1 (7) THIRD PARTY.—The term “third party”
2 means, with respect to a covered entity, a person
3 that—

4 (A) is not related to the covered entity by
5 common ownership or corporate control;

6 (B) is not a service provider used by the
7 covered entity to receive personally identifiable
8 information or sensitive personally identifiable
9 information in performing services or functions
10 on behalf of and under the instruction of the
11 covered entity; and

12 (C) does not have an established business
13 relationship with the individual and does not
14 identify itself to the individual at the time of
15 collection of covered information in a clear and
16 conspicuous manner that is visible to the indi-
17 vidual.

18 (8) UNAUTHORIZED USE.—

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

24 (B) EXCEPTIONS.—Except as provided in
25 subparagraph (C), the term “unauthorized use”

1 does not include use of covered information re-
2 relating to an individual by a covered entity or its
3 service provider as follows:

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

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

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

16 (iv) To investigate a possible crime.

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

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

1 (I) collected directly by the cov-
2 ered entity; or

3 (II) shared with the covered enti-
4 ty—

5 (aa) at the affirmative re-
6 quest of the individual; or

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

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

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

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

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

24 (aa) to improve website
25 navigation and performance; or

1 (bb) to understand and im-
2 prove the interaction of an indi-
3 vidual with the advertising of a
4 covered entity.

5 (ix) Use—

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

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

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

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

1 given the individual in accordance with section
2 201(a)(1).

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

9 **TITLE I—RIGHT TO SECURITY**
10 **AND ACCOUNTABILITY**

11 **SEC. 101. SECURITY.**

12 (a) RULEMAKING REQUIRED.—Not later than 180
13 days after the date of the enactment of this Act, the Com-
14 mission shall initiate a rulemaking proceeding to require
15 each covered entity to carry out security measures to pro-
16 tect the covered information it collects and maintains.

17 (b) PROPORTION.—The requirements prescribed
18 under subsection (a) shall provide for security measures
19 that are proportional to the size, type, and nature of the
20 covered information a covered entity collects.

21 (c) CONSISTENCY.—The requirements prescribed
22 under subsection (a) shall be consistent with guidance pro-
23 vided by the Commission and recognized industry prac-
24 tices for safety and security on the day before the date
25 of the enactment of this Act.

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

4 **SEC. 102. ACCOUNTABILITY.**

5 Each covered entity shall, in a manner proportional
6 to the size, type, and nature of the covered information
7 it collects—

8 (1) have managerial accountability, proportional
9 to the size and structure of the covered entity, for
10 the adoption and implementation of policies con-
11 sistent with this Act;

12 (2) have a process to respond to non-frivolous
13 inquiries from individuals regarding the collection,
14 use, transfer, or storage of covered information re-
15 lating to such individuals; and

16 (3) describe the means of compliance of the cov-
17 ered entity with the requirements of this Act upon
18 request from—

19 (A) the Commission; or

20 (B) an appropriate safe harbor program
21 established under section 501.

22 **SEC. 103. PRIVACY BY DESIGN.**

23 Each covered entity shall, in a manner proportional
24 to the size, type, and nature of the covered information

1 that it collects, implement a comprehensive information
2 privacy program by—

3 (1) incorporating necessary development proc-
4 esses and practices throughout the product life cycle
5 that are designed to safeguard the personally identi-
6 fiable information that is covered information of in-
7 dividuals based on—

8 (A) the reasonable expectations of such in-
9 dividuals regarding privacy; and

10 (B) the relevant threats that need to be
11 guarded against in meeting those expectations;
12 and

13 (2) maintaining appropriate management proc-
14 esses and practices throughout the data life cycle
15 that are designed to ensure that information systems
16 comply with—

17 (A) the provisions of this Act;

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

19 and

20 (C) the privacy preferences of individuals
21 that are consistent with the consent choices and
22 related mechanisms of individual participation
23 as described in section 202.

1 **TITLE II—RIGHT TO NOTICE AND**
2 **INDIVIDUAL PARTICIPATION**

3 **SEC. 201. TRANSPARENT NOTICE OF PRACTICES AND PUR-**
4 **POSES.**

5 (a) IN GENERAL.—Not later than 60 days after the
6 date of the enactment of this Act, the Commission shall
7 initiate a rulemaking proceeding to require each covered
8 entity—

9 (1) to provide clear, concise, and timely notice
10 to individuals of—

11 (A) the practices of the covered entity re-
12 garding the collection, use, transfer, and stor-
13 age of covered information; and

14 (B) the specific purposes of those prac-
15 tices;

16 (2) to provide clear, concise, and timely notice
17 to individuals before implementing a material change
18 in such practices; and

19 (3) to maintain the notice required by para-
20 graph (1) in a form that individuals can readily ac-
21 cess.

22 (b) COMPLIANCE AND OTHER CONSIDERATIONS.—In
23 the rulemaking required by subsection (a), the Commis-
24 sion—

1 (1) shall consider the types of devices and
2 methods individuals will use to access the required
3 notice;

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

10 (3) may draft guidance for covered entities to
11 use in designing their own notice and may include
12 a draft model template for covered entities to use in
13 designing their own notice; and

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

17 **SEC. 202. INDIVIDUAL PARTICIPATION.**

18 (a) IN GENERAL.—Not later than 180 days after the
19 date of the enactment of this Act, the Commission shall
20 initiate a rulemaking proceeding to require each covered
21 entity—

22 (1) to offer individuals a clear and conspicuous
23 mechanism for opt-out consent for any use of their
24 covered information that would otherwise be unau-

1 thorized use, except with respect to any use requir-
2 ing opt-in consent under paragraph (3);

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

7 (3) to offer individuals a clear and conspicuous
8 mechanism for opt-in consent for—

9 (A) the collection, use, or transfer of sen-
10 sitive personally identifiable information other
11 than—

12 (i) to process or enforce a transaction
13 or deliver a service requested by that indi-
14 vidual;

15 (ii) for fraud prevention and detec-
16 tion; or

17 (iii) to provide for a secure physical or
18 virtual environment; and

19 (B) the use of previously collected covered
20 information or transfer to a third party for an
21 unauthorized use of previously collected covered
22 information, if—

23 (i) there is a material change in the
24 covered entity's stated practices that re-
25 quires notice under section 201(a)(2); and

1 (ii) such use or transfer creates a risk
2 of economic or physical harm to an indi-
3 vidual;

4 (4) to provide any individual to whom the per-
5 sonally identifiable information that is covered infor-
6 mation pertains, and which the covered entity or its
7 service provider stores, appropriate and reasonable—

8 (A) access to such information; and

9 (B) mechanisms to correct such informa-
10 tion to improve the accuracy of such informa-
11 tion; and

12 (5) in the case that a covered entity enters
13 bankruptcy or an individual requests the termination
14 of a service provided by the covered entity to the in-
15 dividual or termination of some other relationship
16 with the covered entity, to permit the individual to
17 easily request that—

18 (A) all of the personally identifiable infor-
19 mation that is covered information that the cov-
20 ered entity maintains relating to the individual,
21 except for information the individual authorized
22 the sharing of or which the individual shared
23 with the covered entity in a forum that is wide-
24 ly and publicly available, be rendered not per-
25 sonally identifiable; or

1 (B) if rendering such information not per-
2 sonally identifiable is not possible, to cease the
3 unauthorized use or transfer to a third party
4 for an unauthorized use of such information or
5 to cease use of such information for marketing,
6 unless such unauthorized use or transfer is oth-
7 erwise required by a provision of law.

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

15 (1) specified pursuant to the purposes stated in
16 the required notice under section 201(a); and

17 (2) authorized by the individual when the indi-
18 vidual granted consent for the transfer of the infor-
19 mation to the third party.

20 (c) ALTERNATIVE MEANS TO TERMINATE USE OF
21 COVERED INFORMATION.—In the rulemaking required by
22 subsection (a), the Commission shall allow a covered entity
23 to provide individuals an alternative means, in lieu of the
24 access, consent, and correction requirements, of prohib-

1 iting a covered entity from use or transfer of that individ-
2 ual's covered information.

3 (d) SERVICE PROVIDERS.—

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

14 (A) the requirements of this Act; and

15 (B) the policies and practices related to
16 such information of the covered entity.

17 (2) TRANSFERS BETWEEN SERVICE PROVIDERS
18 FOR A COVERED ENTITY.—The disclosure by a serv-
19 ice provider of covered information pursuant to a
20 contract with a covered entity to another service pro-
21 vider in order to perform the same service or func-
22 tions for that covered entity does not constitute an
23 unauthorized use.

24 (3) LIABILITY REMAINS WITH COVERED ENTI-
25 TY.—A covered entity remains responsible and liable

1 for the protection of covered information that has
2 been transferred to a service provider for processing,
3 notwithstanding any agreement to the contrary be-
4 tween a covered entity and the service provider.

5 **TITLE III—RIGHTS RELATING TO**
6 **DATA MINIMIZATION, CON-**
7 **STRAINTS ON DISTRIBUTION,**
8 **AND DATA INTEGRITY**

9 **SEC. 301. DATA MINIMIZATION.**

10 Each covered entity shall—

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

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

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

21 (C) to prevent or detect fraud or to provide
22 for a secure environment;

23 (D) to investigate a possible crime;

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

1 (F) for the covered entity to market or ad-
2 vertise to such individual if the covered infor-
3 mation used for such marketing or advertising
4 was collected directly by the covered entity;

5 (G) for research and development con-
6 ducted for the improvement of carrying out a
7 transaction or delivering a service; or

8 (H) for internal operations, including—

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

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

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

18 (II) the customer's experience;

19 and

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;

7 (B) with respect to research and develop-
 8 ment described in paragraph (1)(G), is nec-
 9 essary for such research and development; or

10 (C) is required by a provision of law.

11 **SEC. 302. CONSTRAINTS ON DISTRIBUTION OF INFORMA-**
 12 **TION.**

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

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

17 (A) the provisions of this Act; and

18 (B) as specified in the contract;

19 (2) require by contract that such third party
 20 may not combine information that the covered entity
 21 has transferred to it, that relates to an individual,
 22 and that is not personally identifiable information
 23 with other information in order to identify such indi-
 24 vidual, unless the covered entity has obtained the

1 opt-in consent of such individual for such combina-
2 tion and identification; and

3 (3) before executing a contract with a third
4 party—

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

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

10 (b) TRANSFERS TO UNRELIABLE THIRD PARTIES

11 PROHIBITED.—A covered entity may not transfer covered
12 information to a third party that the covered entity
13 knows—

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

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

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

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

22 (2) EXEMPTION.—The Commission may, as it
23 determines appropriate, exempt classes of third par-
24 ties from liability under any provision of title II if
25 the Commission finds that—

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

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

8 **SEC. 303. DATA INTEGRITY.**

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

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

19 (1) directly to the covered entity by the indi-
20 vidual; or

21 (2) to the covered entity by another entity at
22 the request of the individual.

TITLE IV—ENFORCEMENT

2 SEC. 401. GENERAL APPLICATION.

3 The requirements of this Act 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 non-profit organization, including
22 any organization described in section 501(c) of
23 the Internal Revenue code of 1986 that is ex-
24 empt from taxation under section 501(a) of
25 such 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. 402. ENFORCEMENT BY THE FEDERAL TRADE COM-**
8 **MISSION.**

9 (a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—
10 A knowing or repetitive violation of a provision of this Act
11 or a regulation promulgated under this Act shall be treat-
12 ed as an unfair or deceptive act or practice in violation
13 of a regulation under section 18(a)(1)(B) of the Federal
14 Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regard-
15 ing unfair or deceptive acts or practices.

16 (b) POWERS OF COMMISSION.—

17 (1) IN GENERAL.—The Commission shall en-
18 force this Act in the same manner, by the same
19 means, and with the same jurisdiction, powers, and
20 duties as though all applicable terms and provisions
21 of the Federal Trade Commission Act (15 U.S.C. 41
22 et seq.) were incorporated into and made a part of
23 this Act. Any person who violates this Act or the
24 regulations issued under this Act shall be subject to

1 the penalties and entitled to the privileges and im-
2 munities provided in that Act.

3 (2) SPECIAL RULE.—The Commission shall en-
4 force this Act under paragraph (1) of this subsection
5 with respect to common carriers and non-profit or-
6 ganizations described in section 401 to the extent
7 necessary to effectuate the purposes of this Act as
8 if such carriers and non-profit organizations were
9 persons over which the Commission has authority
10 pursuant to section 5(a)(2) of the Federal Trade
11 Commission Act (15 U.S.C. 45(a)(2)).

12 (c) RULEMAKING AUTHORITY.—

13 (1) LIMITATION.—In promulgating rules under
14 this Act, the Commission may not require the de-
15 ployment or use of any specific products or tech-
16 nologies, including any specific computer software or
17 hardware.

18 (2) ADMINISTRATIVE PROCEDURE.—The Com-
19 mission shall promulgate regulations under this Act
20 in accordance with section 553 of title 5, United
21 States Code.

22 **SEC. 403. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

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 Act 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 Act other than title III, the attor-
5 ney general may, as *parens patriae*, bring a civil action
6 on behalf of the residents of the State in an appropriate
7 district court of the United States—

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

11 (2) to compel compliance with this Act or a reg-
12 ulation promulgated under this Act; or

13 (3) for violations of this Act or a regulation
14 promulgated under this Act to obtain civil penalties
15 in the amount determined under section 404.

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 Federal Trade Commis-
22 sion in writing of any civil action under sub-
23 section (b), prior to 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 Federal
11 Trade Commission 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 Federal Trade Commission institutes a
20 civil action for violation of this Act or a regulation promul-
21 gated under this Act, no attorney general of a State may
22 bring a civil action under subsection (a) against any de-
23 fendant named in the complaint of the Commission for
24 violation of this Act or a regulation promulgated under
25 this Act that is 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 **SEC. 404. CIVIL PENALTIES.**

9 (a) IN GENERAL.—In an action brought under sec-
10 tion 403, in addition to any other penalty otherwise appli-
11 cable to a violation of this Act or any regulation promul-
12 gated under this Act, the following civil penalties shall
13 apply:

14 (1) TITLE I VIOLATIONS.—A covered entity that
15 knowingly or repeatedly violates title I is liable for
16 a civil penalty equal to the amount calculated by
17 multiplying the number of days that the entity is not
18 in compliance with such title by an amount not to
19 exceed \$16,500.

20 (2) TITLE II VIOLATIONS.—A covered entity
21 that knowingly or repeatedly violates title II is liable
22 for a civil penalty equal to the amount calculated by
23 multiplying the number of days that such an entity
24 is not in compliance with such title, or the number
25 of individuals for whom the entity failed to obtain

1 consent as required by such title, whichever is great-
2 er, by an amount not to exceed \$16,500.

3 (b) ADJUSTMENT FOR INFLATION.—Beginning on
4 the date that the Consumer Price Index for All Urban
5 Consumers is first published by the Bureau of Labor Sta-
6 tistics that is after 1 year after the date of the enactment
7 of this Act, and each year thereafter, each of the amounts
8 specified in subsection (a) shall be increased by the per-
9 centage increase in the Consumer Price Index published
10 on that date from the Consumer Price Index published
11 the previous year.

12 (c) MAXIMUM TOTAL LIABILITY.—Notwithstanding
13 the number of actions which may be brought against a
14 covered entity under section 403, the maximum civil pen-
15 alty for which any covered entity may be liable under this
16 section in such actions shall not exceed—

17 (1) \$3,000,000 for any related series of viola-
18 tions of any rule promulgated under title I; and

19 (2) \$3,000,000 for any related series of viola-
20 tions of title II.

21 **SEC. 405. EFFECT ON OTHER LAWS.**

22 (a) PREEMPTION OF STATE LAWS.—The provisions
23 of this Act shall supersede any provisions of the law of
24 any State relating to those entities covered by the regula-

1 tions issued pursuant to this Act, to the extent that such
 2 provisions relate to the collection, use, or disclosure of—

3 (1) covered information addressed in this Act;

4 or

5 (2) personally identifiable information or per-
 6 sonal identification information addressed in provi-
 7 sions of the law of a State.

8 (b) UNAUTHORIZED CIVIL ACTIONS; CERTAIN STATE
 9 LAWS.—

10 (1) UNAUTHORIZED ACTIONS.—No person
 11 other than a person specified in section 403 may
 12 bring a civil action under the laws of any State if
 13 such action is premised in whole or in part upon the
 14 defendant violating this Act or a regulation promul-
 15 gated under this Act.

16 (2) PROTECTION OF CERTAIN STATE LAWS.—
 17 This Act shall not be construed to preempt the ap-
 18 plicability of—

19 (A) State laws that address the collection,
 20 use, or disclosure of health information or fi-
 21 nancial information;

22 (B) State laws that address notification re-
 23 quirements in the event of a data breach; or

24 (C) other State laws to the extent that
 25 those laws relate to acts of fraud.

1 (c) RULE OF CONSTRUCTION RELATING TO RE-
 2 QUIRED DISCLOSURES TO GOVERNMENT ENTITIES.—
 3 This Act shall not be construed to expand or limit the
 4 duty or authority of a covered entity or third party to dis-
 5 close personally identifiable information to a government
 6 entity under any provision of law.

7 **SEC. 406. NO PRIVATE RIGHT OF ACTION.**

8 This Act may not be construed to provide any private
 9 right of action.

10 **TITLE V—CO-REGULATORY SAFE**
 11 **HARBOR PROGRAMS**

12 **SEC. 501. ESTABLISHMENT OF SAFE HARBOR PROGRAMS.**

13 (a) IN GENERAL.—Not later than 365 days after the
 14 date of the enactment of this Act, the Commission shall
 15 initiate a rulemaking proceeding to establish requirements
 16 for the establishment and administration of safe harbor
 17 programs under which a nongovernmental organization
 18 will administer a program that—

19 (1) establishes a mechanism for participants to
 20 implement the requirements of this Act with regards
 21 to—

22 (A) certain types of unauthorized uses of
 23 covered information as described in paragraph
 24 (2); or

1 (B) any unauthorized use of covered infor-
 2 mation; and

3 (2) offers consumers a clear, conspicuous, per-
 4 sistent, and effective means of opting out of the
 5 transfer of covered information by a covered entity
 6 participating in the safe harbor program to a third
 7 party for—

8 (A) behavioral advertising purposes;

9 (B) location-based advertising purposes;

10 (C) other specific types of unauthorized
 11 use; or

12 (D) any unauthorized use.

13 (b) SELECTION OF NONGOVERNMENTAL ORGANIZA-
 14 TIONS TO ADMINISTER PROGRAM.—

15 (1) SUBMITTAL OF APPLICATIONS.—An appli-
 16 cant seeking to administer a program under the re-
 17 quirements established pursuant to subsection (a)
 18 shall submit to the Commission an application there-
 19 for at such time, in such manner, and containing
 20 such information as the Commission may require.

21 (2) NOTICE AND RECEIPT OF APPLICATIONS.—
 22 Upon completion of the rulemaking proceedings re-
 23 quired by subsection (a), the Commission shall—

24 (A) publish a notice in the Federal Reg-
 25 ister that it will receive applications for ap-

1 proval of safe harbor programs under this title;
2 and

3 (B) begin receiving applications under
4 paragraph (1).

5 (3) SELECTION.—Not later than 270 days after
6 the date on which the Commission receives a com-
7 pleted application under this subsection, the Com-
8 mission shall grant or deny the application on the
9 basis of the Commission’s evaluation of the appli-
10 cant’s capacity to provide protection of individuals’
11 covered information with regard to specific types of
12 unauthorized uses of covered information as de-
13 scribed in subsection (a)(2) that is substantially
14 equivalent to or superior to the protection otherwise
15 provided under this Act.

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

20 (c) SCOPE OF SAFE HARBOR PROTECTION.—The
21 scope of protection offered by safe harbor programs ap-
22 proved by the Commission that establish mechanisms for
23 participants to implement the requirements of the Act only
24 for certain uses of covered information as described in

1 subsection (a)(2) shall be limited to participating entities'
2 use of those particular types of covered information.

3 (d) SUPERVISION BY FEDERAL TRADE COMMIS-
4 SION.—

5 (1) IN GENERAL.—The Commission shall exer-
6 cise oversight and supervisory authority of a safe
7 harbor program approved under this section
8 through—

9 (A) ongoing review of the practices of the
10 nongovernmental organization administering
11 the program;

12 (B) the imposition of civil penalties on the
13 nongovernmental organization if it is not com-
14 pliant with the requirements established under
15 subsection (a); and

16 (C) withdrawal of authorization to admin-
17 ister the safe harbor program under this title.

18 (2) ANNUAL REPORTS BY NONGOVERNMENTAL
19 ORGANIZATIONS.—Each year, each nongovernmental
20 organization administering a safe harbor program
21 under this section shall submit to the Commission a
22 report on its activities under this title during the
23 preceding year.

1 **SEC. 502. PARTICIPATION IN SAFE HARBOR PROGRAM.**

2 (a) EXEMPTION.—Any covered entity that partici-
3 pates in, and demonstrates compliance with, a safe harbor
4 program administered under section 501 shall be exempt
5 any provision of title II or title III if the Commission finds
6 that the requirements of the safe harbor program are sub-
7 stantially the same as or more protective of privacy of in-
8 dividuals than the requirements of the provision from
9 which the exemption is granted.

10 (b) LIMITATION.—Nothing in this title shall be con-
11 strued to exempt any covered entity participating in a safe
12 harbor program from compliance with any other require-
13 ment of the regulations promulgated under this Act for
14 which the safe harbor does not provide an exception.

15 **TITLE VI—APPLICATION WITH**
16 **OTHER FEDERAL LAWS**

17 **SEC. 601. APPLICATION WITH OTHER FEDERAL LAWS.**

18 (a) QUALIFIED EXEMPTION FOR PERSONS SUBJECT
19 TO OTHER FEDERAL PRIVACY LAWS.—If a person is sub-
20 ject to a provision of this Act and a provision of a Federal
21 privacy law described in subsection (d), such provision of
22 this Act shall not apply to such person to the extent that
23 such provision of Federal privacy law applies to such per-
24 son.

25 (b) PROTECTION OF OTHER FEDERAL PRIVACY
26 LAWS.—Nothing in this Act may be construed to modify,

1 limit, or supersede the operation of the Federal privacy
2 laws described in subsection (d) or the provision of infor-
3 mation permitted or required, expressly or by implication,
4 by such laws, with respect to Federal rights and practices.

5 (c) COMMUNICATIONS INFRASTRUCTURE AND PRI-
6 VACY.—If a person is subject to a provision of section 222
7 or 631 of the Communications Act of 1934 (47 U.S.C.
8 222 and 551) and a provision of this Act, such provision
9 of such section 222 or 631 shall not apply to such person
10 to the extent that such provision of this Act applies to
11 such person.

12 (d) OTHER FEDERAL PRIVACY LAWS DESCRIBED.—
13 The Federal privacy laws described in this subsection are
14 as follows:

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

17 (2) The Right to Financial Privacy Act of 1978
18 (12 U.S.C. 3401 et seq.).

19 (3) The Fair Credit Reporting Act (15 U.S.C.
20 1681 et seq.).

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

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

1 (6) Title V of the Gramm-Leach-Bliley Act of
2 1999 (15 U.S.C. 6801 et seq.).

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

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

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

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

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

15 (12) The regulations promulgated under section
16 264(c) of the Health Insurance Portability and Ac-
17 countability Act of 1996 (42 U.S.C. 1320d–2 note),
18 as such regulations relate to a person described in
19 section 1172(a) of the Social Security Act (42
20 U.S.C. 1320d–1(a)) or to transactions referred to in
21 section 1173(a)(1) of such Act (42 U.S.C. 1320d–
22 2(a)(1)).

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

1 (14) Section 227 of the Communications Act of
2 1934 (47 U.S.C. 227).

3 **TITLE VII—DEVELOPMENT OF**
4 **COMMERCIAL DATA PRIVACY**
5 **POLICY IN THE DEPARTMENT**
6 **OF COMMERCE**

7 **SEC. 701. DIRECTION TO DEVELOP COMMERCIAL DATA PRI-**
8 **VACY POLICY.**

9 The Secretary of Commerce shall contribute to the
10 development of commercial data privacy policy by—

11 (1) convening private sector stakeholders, in-
12 cluding members of industry, civil society groups,
13 academia, in open forums, to develop codes of con-
14 duct in support of applications for safe harbor pro-
15 grams under title V;

16 (2) expanding interoperability between the
17 United States commercial data privacy framework
18 and other national and regional privacy frameworks;

19 (3) conducting research related to improving
20 privacy protection under this Act; and

21 (4) conducting research related to improving
22 data sharing practices, including the use of
23 anonymised data, and growing the information econ-
24 omy.

○