

109TH CONGRESS  
1ST SESSION

# H. R. 1263

To protect and enhance consumer privacy, and for other purposes.

---

## IN THE HOUSE OF REPRESENTATIVES

MARCH 10, 2005

Mr. STEARNS introduced the following bill; which was referred to the Committee on Energy and Commerce, and in addition to the Committee on International Relations, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

## A BILL

To protect and enhance consumer privacy, and for other purposes.

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

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Consumer Privacy Pro-  
5 tection Act of 2005”.

6 **SEC. 2. TABLE OF CONTENTS.**

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

- Sec. 1. Short title.
- Sec. 2. Table of contents.
- Sec. 3. Definitions.

TITLE I—PROTECTION OF INDIVIDUAL PRIVACY IN INTERSTATE  
COMMERCE

- Sec. 101. Privacy notices to consumers.
- Sec. 102. Privacy policy statements.
- Sec. 103. Consumer opportunity to limit sale or disclosure of information.
- Sec. 104. Consumer opportunity to limit other information practices.
- Sec. 105. Information security obligations.
- Sec. 106. Self-regulatory programs.
- Sec. 107. Enforcement.
- Sec. 108. No private right of action.
- Sec. 109. Effect on other laws.
- Sec. 110. Effective date.

TITLE II—IDENTITY THEFT PREVENTION AND REMEDIES

- Sec. 201. Facilitating electronic identity theft affidavits.
- Sec. 202. Promoting use of common identity theft affidavit.
- Sec. 203. Timely resolution of identity theft disputes.
- Sec. 204. Improvements to consumer clearinghouse.
- Sec. 205. Improved identity theft data.
- Sec. 206. Change of address protections.
- Sec. 207. Effective date.

TITLE III—INTERNATIONAL PROVISIONS

- Sec. 301. Study by Comptroller General.
- Sec. 302. Remediation of discriminatory impact by Secretary of Commerce.
- Sec. 303. Effect of nonremediation.
- Sec. 304. Harmonization of international privacy laws, regulations, and agreements.

1 **SEC. 3. DEFINITIONS.**

2 In this Act:

3 (1) The term “Commission” means the Federal  
4 Trade Commission.

5 (2) The term “consumer” means an individual  
6 acting in the individual’s personal, family, or house-  
7 hold capacity.

8 (3)(A) The term “data collection organization”  
9 means an entity (or an agent or affiliate of the enti-  
10 ty) that collects (by any means, through any me-

1       dium), sells, discloses for consideration, or uses per-  
2       sonally identifiable information of the consumer.

3           (B) Such term does not include—

4               (i) a governmental agency;

5               (ii) a not-for-profit entity, to the extent  
6       that personally identifiable information is not  
7       used for a commercial purpose;

8               (iii) an entity that—

9                   (I) has annual gross revenue under  
10       \$1,000,000 (based on the value of such  
11       amount in fiscal year 2000, adjusted for  
12       current dollars);

13                   (II) has fewer than 25 employees;

14                   (III) collects or uses personally identi-  
15       fiable information from fewer than 1,000  
16       consumers for a purpose unrelated to a  
17       transaction with the consumer;

18                   (IV) does not process personally iden-  
19       tifiable information of consumers; and

20                   (V) does not sell or disclose for con-  
21       sideration such information to another per-  
22       son;

23               (iv) a provider of professional services, or  
24       any affiliate thereof, to the extent that such  
25       provider is obligated by rules of professional

1 ethics, or by applicable law or regulation, not to  
2 voluntarily disclose confidential client informa-  
3 tion without the consent of the client; or

4 (v) a data processing outsourcing entity.

5 (4)(A) The term “personally identifiable infor-  
6 mation”, with respect to a data collection organiza-  
7 tion means individually identifiable information re-  
8 lating to a living individual who can be identified  
9 from that information.

10 (B) Such term includes—

11 (i) first and last name, whether given at  
12 birth or adoption, assumed, or legally changed;

13 (ii) home or other physical address includ-  
14 ing street name and name of a city or town;

15 (iii) electronic mail address;

16 (iv) telephone number;

17 (v) social security number; or

18 (vi) any other unique identifying informa-  
19 tion that a data collector and processor collects  
20 and combines with any information described in  
21 the preceding subparagraphs of this paragraph.

22 (C) Such term does not include—

23 (i) anonymous or aggregate data, or any  
24 other information that does not identify a  
25 unique living individual;

1 (ii) information about a consumer inferred  
2 from data maintained about a consumer; or

3 (iii) information about a consumer ob-  
4 tained from a public record.

5 (5) The term “affiliate” means any company  
6 that controls, is controlled by, or is under common  
7 control with another company.

8 (6) The term “information-sharing affiliate”  
9 means any affiliate that is under common control  
10 with a data collection organization, and is contrac-  
11 tually obligated to comply with the practices enu-  
12 merated under the privacy policy statement of the  
13 organization required under section 102.

14 (7) The term “data processing outsourcing enti-  
15 ty” means, with respect to a data collection organi-  
16 zation, a non-affiliated entity that—

17 (A) provides information technology proc-  
18 essing, Web hosting, or telecommunications  
19 services to the data collection organization;

20 (B) is contractually obligated to comply  
21 with security controls specified by the data col-  
22 lection organization; and

23 (C) has no right to use the data collection  
24 organization’s personally identifiable informa-  
25 tion other than for performing data processing

1           outsourcing services for the data collection or-  
2           ganization or as required by law.

3           (8) The term “process”, with respect to person-  
4           ally identifiable information, means any value-added  
5           activity performed on data by automated means.

6           (9) The term “transaction” means an inter-  
7           action between a consumer and a data collection or-  
8           ganization resulting in—

9                   (A) any use of information that is nec-  
10                  essary to complete the interaction in the course  
11                  of which information is collected, or to maintain  
12                  the provisioning of a good or service requested  
13                  by the consumer, including use—

14                           (i) to approve, guarantee, process, ad-  
15                           minister, complete, enforce, provide, or  
16                           market a product, service, account, benefit,  
17                           transaction, or payment method that is re-  
18                           quested or approved by the consumer; or

19                           (ii) to deliver goods, services, funds,  
20                           or other consideration to, or on behalf of,  
21                           the consumer;

22                   (B) any disclosure of information that is  
23                  necessary for the consumer to enforce any right  
24                  of the consumer;

1 (C) any disclosure of information that is  
2 required by law or by a court order; and

3 (D) any use of information to verify per-  
4 sonally identifiable information by the con-  
5 sumer, evaluate, detect, or reduce the risk of  
6 fraud or other criminal activity, or other risk-  
7 management activities.

8 (10) The term “display” means intentionally  
9 communicating or otherwise making available (on  
10 the Internet or in any other manner) to another per-  
11 son.

12 (11) The term “public record” means any item,  
13 collection, or grouping of information about an indi-  
14 vidual that is maintained by a Federal, State, or  
15 local government entity and that is made available  
16 to the public.

17 (12) The term “purchase” means providing, di-  
18 rectly or indirectly, anything of value in exchange  
19 for a good or service.

20 (13) The term “State” includes the several  
21 States, the District of Columbia, the Commonwealth  
22 of Puerto Rico, the Commonwealth of the Northern  
23 Mariana Islands, American Samoa, Guam, the Vir-  
24 gin Islands, the Freely Associated States, and any  
25 other territory or possession of the United States.

1 **TITLE I—PROTECTION OF INDI-**  
2 **VIDUAL PRIVACY IN INTER-**  
3 **STATE COMMERCE**

4 **SEC. 101. PRIVACY NOTICES TO CONSUMERS.**

5 (a) NOTICE REQUIRED.—A data collection organiza-  
6 tion shall provide to a consumer a notice containing the  
7 information required under subsection (b) as follows:

8 (1) Upon the first instance of collection from  
9 the consumer of personally identifiable information,  
10 that may be used for a purpose unrelated to the  
11 transaction, by a data collection organization, the or-  
12 ganization shall provide the notice at the time per-  
13 sonally identifiable information is collected.

14 (2) Upon a material change in the organiza-  
15 tion's privacy policy under section 102(a), the orga-  
16 nization shall provide the notice, not later than the  
17 first time after such change in policy that the orga-  
18 nization seeks to collect, sell, disclose for consider-  
19 ation, or use personally identifiable information to  
20 the extent practicable, to each consumer from whom  
21 the organization has collected such information.

22 (b) FORM AND CONTENTS OF NOTICE.—A notice re-  
23 quired under subsection (a) shall be provided in a clear  
24 and conspicuous manner, be prominently displayed or ex-

1 plicitly stated to the consumer, and contain the following  
2 information:

3           (1) A statement that the personal information  
4           collected by the data collection organization may be  
5           used or disclosed for purposes or transactions unre-  
6           lated to that for which it was collected, as described  
7           in the organization’s privacy statement.

8           (2) A description of the manner in which the  
9           consumer may obtain a privacy policy statement that  
10          meets the requirements of section 102, which may  
11          include providing the consumer with an Internet  
12          website, a hyperlink to such a website, or a toll-free  
13          telephone number from which such a statement may  
14          be obtained. If the notice required under subsection  
15          (a) is provided to the consumer by means of an  
16          Internet website, one manner in which the consumer  
17          may obtain the privacy policy statement must be by  
18          means of an Internet website.

19          (3) If the notice is required under subsection  
20          (a)(2), a statement that there has been a material  
21          change in the organization’s privacy policy.

22 **SEC. 102. PRIVACY POLICY STATEMENTS.**

23          (a) **PRIVACY POLICY.**—A data collection organization  
24          shall establish a privacy policy with respect to the collec-  
25          tion, sale, disclosure for consideration, dissemination, use,

1 and security of the personally identifiable information of  
2 consumers, the principal elements of which shall be em-  
3 bodied in a privacy policy statement (or statements) that  
4 meets the requirements of subsection (b).

5 (b) STATEMENT.—The statement (or statements) re-  
6 quired under subsection (a) shall meet the following re-  
7 quirements:

8 (1) The statement must be brief, concise, clear,  
9 and conspicuous and written in plain language.

10 (2) The statement must be accessible to all con-  
11 sumers of the data collection organization (regard-  
12 less of the means by which a consumer conducts a  
13 transaction with the organization)—

14 (A) at no charge to the consumer; and

15 (B) at the time the data collection organi-  
16 zation first collects personally identifiable infor-  
17 mation about the consumer that may be used  
18 for a purpose unrelated to a transaction with  
19 the consumer and subsequently.

20 (3) The statement must disclose only the fol-  
21 lowing:

22 (A) The identity of each data collection or-  
23 ganization, or a description of each class or  
24 type of data collection organization, that may  
25 collect or use the information.

1 (B) The types of information that may be  
2 collected or used.

3 (C) How the information may be used.

4 (D) Whether the consumer is required to  
5 provide the information in order to do business  
6 with the data collection organization.

7 (E) The extent to which the information is  
8 subject to sale or disclosure for consideration to  
9 a data collection organization that is not an in-  
10 formation-sharing affiliate of the data collection  
11 organization providing the statement, includ-  
12 ing—

13 (i) a clear and prominent statement of  
14 the fact that the information is subject to  
15 such sale or disclosure for consideration;

16 (ii) a description of each class or type  
17 of data collection organization to which the  
18 information may be sold or disclosed for  
19 consideration;

20 (iii) to the extent practicable, the pur-  
21 pose for which the information may be  
22 used; and

23 (iv) the types of information that may  
24 be sold or disclosed for consideration.

1 (F) Whether the information security prac-  
2 tices of the data collection organization meet  
3 the security requirements of section 105 in  
4 order to prevent unauthorized disclosure or re-  
5 lease of personally identifiable information.

6 (c) COMMISSION FACILITATION.—The Commission  
7 shall take actions (including conducting industry-wide  
8 workshops) to facilitate the development of harmonized,  
9 universal wording or logo-based graphics in order to con-  
10 vey the contents of privacy policy statements required  
11 under this section.

12 **SEC. 103. CONSUMER OPPORTUNITY TO LIMIT SALE OR DIS-**  
13 **CLOSURE OF INFORMATION.**

14 (a) PRECLUSION OF SALE OR DISCLOSURE.—

15 (1) REQUIREMENT.—A data collection organi-  
16 zation shall provide to the consumer, without charge,  
17 the opportunity to preclude any sale or disclosure for  
18 consideration of the consumer’s personally identifi-  
19 able information, provided in a particular data col-  
20 lection, that may be used for a purpose other than  
21 a transaction with the consumer, to any data collec-  
22 tion organization that is not an information-sharing  
23 affiliate of the data collection organization providing  
24 such opportunity.



1           (1) a notice and description of such opportunity  
2 must appear in the privacy statement;

3           (2) such opportunity must be easy to access  
4 and to use; and

5           (3) any limitation exercised by the consumer  
6 pursuant to such opportunity shall remain in effect,  
7 unless—

8                 (A) the limitation is withdrawn by the con-  
9 sumer; or

10                (B) the data collection organization pro-  
11 vides the consumer at least 30 days notice be-  
12 fore materially changing the limitation or termi-  
13 nating its compliance with the limitation.

14 **SEC. 105. INFORMATION SECURITY OBLIGATIONS.**

15         (a) INFORMATION SECURITY POLICY.—

16                 (1) IMPLEMENTATION.—A data collection orga-  
17 nization shall prepare, revise as necessary, and im-  
18 plement an information security policy that is appli-  
19 cable to the information security practices and treat-  
20 ment of personally identifiable information main-  
21 tained by the data collection organization, that is de-  
22 signed to prevent the unauthorized disclosure or re-  
23 lease of such information.

24                 (2) MANAGEMENT APPROVAL.—An information  
25 security policy created pursuant to paragraph (1)

1 shall be considered and approved by the senior man-  
2 agement officials of the data collection organization.

3 (3) CONTENTS.—An information security policy  
4 required under paragraph (1) shall include—

5 (A) a process for taking corrective action  
6 pursuant to subsection (b); and

7 (B) identifying an officer of the data col-  
8 lection organization as the point of contact with  
9 responsibility for information security issues for  
10 the organization.

11 (b) CORRECTIVE ACTIONS.—

12 (1) INFORMATION SECURITY ADVISORIES AND  
13 ACTION.—Except as provided in paragraph (2), upon  
14 the issuance of an information security advisory (as  
15 such term is defined in subsection (d)), a data col-  
16 lection organization shall, within a reasonable period  
17 of time after the issuance of such advisory and pur-  
18 suant to its information security policy, take appro-  
19 priate action reasonably necessary to mitigate  
20 against any vulnerability identified in such advisory,  
21 including implementing any changes to its security  
22 practices and the architecture, installation, or imple-  
23 mentation of its network or operating software (in-  
24 cluding corrective patches) in response to such advi-  
25 sory.

1           (2) EXCEPTIONS.—A data collection organiza-  
2           tion shall not be required to take the action specified  
3           in an information security advisory under paragraph  
4           (1) if such organization can, in good faith, show  
5           that—

6                   (A) the corrective action required would  
7                   cause harm to, or weaken, the organization’s  
8                   existing information security for personally  
9                   identifiable information or the procedures or  
10                  systems of the organization;

11                   (B) the organization takes, or has taken,  
12                   other appropriate steps or corrective action to  
13                   mitigate the vulnerabilities and exposure risks  
14                   identified in the information security advisory;  
15                  or

16                   (C) the specified corrective action is not  
17                  necessary.

18           (c) EFFECT OF RELEASE OF PERSONALLY IDENTIFI-  
19           ABLE INFORMATION.—If the security of a data collection  
20           organization has been compromised, resulting in the unau-  
21           thorized release of a consumer’s personally identifiable in-  
22           formation, the data collection organization shall be pre-  
23           sumed to be in violation of this section if such organization  
24           has failed to respond to an information security advisory  
25           in accordance with subsection (b)(1).

1 (d) DEFINITION.—As used in this section, the term  
2 “information security advisory” means an information se-  
3 curity advisory issued by the Federal Computer Incident  
4 Response Center of the Department of Homeland Secu-  
5 rity, or its successor agency.

6 **SEC. 106. SELF-REGULATORY PROGRAMS.**

7 (a) SELF-REGULATORY PROGRAM.—

8 (1) PRESUMPTION OF COMPLIANCE.—The Com-  
9 mission shall presume that a data collection organi-  
10 zation is in compliance with the provisions of sec-  
11 tions 101 through 105 if that organization—

12 (A) participates in a self-regulatory pro-  
13 gram approved under subsection (b); and

14 (B) has been determined by a self-regu-  
15 latory program to be in compliance with the  
16 guidelines, procedures, requirements, and re-  
17 strictions of the program (including a remedial  
18 process under subsection (c)(7)).

19 (2) EFFECT OF WILLFUL NONCOMPLIANCE.—A  
20 data collection organization that participates in a  
21 self-regulatory program under this section shall not  
22 be liable for a civil penalty arising out of a violation  
23 of any provision of sections 101 through 105 unless  
24 such violation results from willful noncompliance

1 with the guidelines, procedures, requirements, or re-  
2 strictions of the program.

3 (b) APPROVAL BY COMMISSION.—

4 (1) APPROVAL.—The Commission shall, within  
5 90 days after submission of an application for ap-  
6 proval of a self-regulatory program under this sec-  
7 tion (or of a material change in a program pre-  
8 viously approved by the Commission), approve such  
9 program (or change) if the Commission finds that  
10 the program (or change) complies with the require-  
11 ments of subsection (c).

12 (2) FORM OF APPLICATION.—The Commission  
13 shall accept an application for approval under para-  
14 graph (1) in any reasonable form the applicant may  
15 submit.

16 (3) DURATION UNTIL RENEWAL.—A self-regu-  
17 latory program approved by the Commission under  
18 paragraph (1) shall be approved for a period of 5  
19 years.

20 (4) REVOCATION OF APPROVAL.—The Commis-  
21 sion may, after notice and opportunity for a hearing,  
22 revoke approval granted under paragraph (1), if the  
23 Commission finds that a self-regulatory program  
24 fails to meet the requirements of subsection (c).

1           (5) JUDICIAL REVIEW.—Any order by the Com-  
2           mission denying approval of a self-regulatory pro-  
3           gram shall be subject to judicial review, as provided  
4           in section 706 of title 5, United States Code.

5           (c) REQUIREMENTS OF SELF-REGULATORY PRO-  
6           GRAM.—A self-regulatory program complies with the re-  
7           quirements of this subsection if the program provides each  
8           of the following:

9           (1) Guidelines and procedures requiring a pro-  
10          gram participant to provide substantially equivalent  
11          or greater protections for consumers and their per-  
12          sonally identifiable information as are provided  
13          under sections 101 through 105.

14          (2) Procedures and requirements to provide  
15          for—

16                (A) an initial review of a participant’s pri-  
17                vacy statement and privacy policy, and subse-  
18                quent review whenever such statement or policy  
19                is substantively changed, to determine whether  
20                the participant complies with the self-regulatory  
21                program’s guidelines;

22                (B) an initial self-review and self-certifi-  
23                cation of a participant’s privacy policy and  
24                practices to ensure compliance with the guide-  
25                lines, procedures, requirements, and restrictions

1 of the program established under this sub-  
2 section;

3 (C) subsequent periodic self-reviews and  
4 self-certifications, which shall occur at least an-  
5 nually, of the participant's privacy policy and  
6 practices to ensure continued compliance with  
7 such guidelines, procedures, requirements, and  
8 restrictions;

9 (D) submission of self-reviews and self-cer-  
10 tifications under this paragraph to any adminis-  
11 trator of the program; and

12 (E) random compliance testing of partici-  
13 pants, which may concentrate on selected com-  
14 pliance issues, if the self-regulatory program  
15 conducts—

16 (i) a random compliance test with re-  
17 spect to each participant not less fre-  
18 quently than every 3 years;

19 (ii) a full compliance test in any case  
20 where non-compliance with any of the se-  
21 lected compliance issues is identified; and

22 (iii) full compliance tests of partici-  
23 pants with a high number of complaints  
24 against them.

1           (3) Procedures and requirements that ensure  
2           that a program participant provides a process for re-  
3           solving disputes with consumers relating to the pri-  
4           vacy policy and practices of the participant. Such  
5           dispute resolution process—

6                   (A) must be available without charge to a  
7           consumer;

8                   (B) must be available at a cost to the par-  
9           ticipant that is reasonable and does not discour-  
10          age participation by the participant in such  
11          process;

12                  (C) must ensure that consumers are in-  
13          formed of how to utilize the process;

14                  (D) may include, as one choice among oth-  
15          ers, binding arbitration; and

16                  (E)(i) must be completed within 60 days  
17          after submission of the dispute by the con-  
18          sumer; or

19                  (ii) must be completed within 90 days after  
20          submission of the dispute by the consumer, if  
21          the participant—

22                   (I) determines that additional time is  
23                  required to obtain information to make an  
24                  informed decision with respect to the dis-  
25                  pute; and

1 (II) notifies the consumer and the  
2 self-regulatory program that such addi-  
3 tional time is required.

4 (4) Provisions for the use by participants in the  
5 program of a means (including the use of a seal) to  
6 represent the participant's participation in the pro-  
7 gram.

8 (5) With respect to any nonvoluntary suspen-  
9 sion or termination of participation in the program  
10 because of the participant's failure to comply with  
11 the program, procedures or requirements to provide  
12 for the following:

13 (A) Publication of notice and the reasons  
14 for any such suspension or termination, except  
15 that no personally identifiable information re-  
16 lated to such suspension or termination may be  
17 published.

18 (B) Notice to the Commission of any such  
19 termination.

20 (6) Requirements and restrictions that assure  
21 independence with respect to program eligibility,  
22 compliance, and dispute resolution mechanisms and  
23 decisions from improper interference by management  
24 or ownership of the self-regulatory program partici-  
25 pant.

1           (7) A process for a noncompliant participant to  
2 take timely remedial action in order to come back  
3 into compliance with the program before suspension  
4 or termination of participation in the program.

5 (d) CONSUMER DISPUTE RESOLUTION.—

6           (1) SELF-REGULATORY DISPUTE PROCESS.—If  
7 a consumer has a dispute with a participant in a  
8 self-regulatory program under this section or under  
9 section 5 of the Federal Trade Commission Act (15  
10 U.S.C. 45) to the extent that such dispute pertains  
11 to the entity’s privacy policy or practices required  
12 for participation in the self-regulatory program, the  
13 consumer shall initially seek resolution through the  
14 participant’s dispute resolution process (established  
15 in accordance with subsection (c)(3)). The Commis-  
16 sion shall promptly refer to the participant involved  
17 any dispute submitted to the Commission for which  
18 resolution has not been initially sought through such  
19 process.

20           (2) RESOLUTION BY COMMISSION.—A consumer  
21 may submit to the Commission for resolution a dis-  
22 pute with a participant in a self-regulatory program  
23 under this section, if the following requirements are  
24 met:

1 (A) The dispute was initially submitted  
2 under paragraph (1) for resolution through the  
3 participant's dispute resolution process.

4 (B) The dispute submitted under para-  
5 graph (1) is not resolved—

6 (i) within 60 days after submission of  
7 the dispute by the consumer; or

8 (ii) to the satisfaction of the con-  
9 sumer.

10 (C) Notice of the facts of the dispute is  
11 submitted to the Commission not later than 30  
12 days after the date on which the consumer is  
13 notified of the resolution through the partici-  
14 pant's dispute resolution process.

15 (D) The consumer has not voluntarily ac-  
16 cepted a resolution of the dispute under para-  
17 graph (1).

18 (E) The dispute was not resolved through  
19 binding arbitration.

20 (3) LIMITATION.—Nothing in this Act shall  
21 prevent the Commission from investigating compli-  
22 ance with this Act by a participant in a self-regu-  
23 latory organization based upon a complaint from an  
24 individual or organization other than a consumer  
25 with a dispute with such participant, or on its own

1 initiative, except that prior to instituting any such  
2 investigation the Commission shall afford the self-  
3 regulatory organization a reasonable opportunity to  
4 invoke its own remedial procedures and assure com-  
5 pliance by the participant.

6 (4) CLEAR AND CONVINCING EVIDENCE.—The  
7 presumption established by paragraph (1) of sub-  
8 section (a) may be overcome by clear and convincing  
9 evidence of non-compliance.

10 (e) NONRELEASE OF CERTAIN INFORMATION.—The  
11 Commission may not compel a participant in a self-regu-  
12 latory program approved under subsection (b) (or an ad-  
13 ministrator of such a program) to provide proprietary in-  
14 formation or personally identifiable information of con-  
15 sumers to the Commission unless the Commission provides  
16 assurances that such information will not be released to  
17 the public.

18 (f) MISREPRESENTATION OF SELF-REGULATORY  
19 PROGRAM PARTICIPATION.—It is unlawful for a data col-  
20 lection organization to misrepresent that it is a participant  
21 in a self-regulatory program (including through any mech-  
22 anism provided under subsection (c)(4)) when such orga-  
23 nization is not, in fact, such a participant.

24 (g) EXEMPTED ENTITY PARTICIPATION.—An entity  
25 that is not a data collection organization and that volun-

1 tarily participates in a self-regulatory program under this  
2 section shall enjoy the rights and benefits provided under  
3 this section in any action or investigation under section  
4 5 of the Federal Trade Commission Act (15 U.S.C. 45)  
5 to the extent that such action or investigation pertains to  
6 the entity's privacy policy or practices required for partici-  
7 pation in the self-regulatory program.

8 **SEC. 107. ENFORCEMENT.**

9 (a) UNFAIR OR DECEPTIVE ACT OR PRACTICE.—A  
10 violation of any provision of this title by a data collection  
11 organization is an unfair or deceptive act or practice un-  
12 lawful under section 5(a)(1) of the Federal Trade Com-  
13 mission Act (15 U.S.C. 45(a)(1)), except that the amount  
14 of any civil penalty under such Act shall be doubled for  
15 a violation of this title, but may not exceed \$500,000 for  
16 all related violations by a single violator (without respect  
17 to the number of consumers affected or the duration of  
18 the related violations).

19 (b) GUIDELINES AND OPINIONS.—In order to assist  
20 in compliance with this title, the Federal Trade Commis-  
21 sion may promulgate regulations and interpretive rules  
22 under section 18 of the Federal Trade Commission Act  
23 (15 U.S.C. 57a), with respect to specific types of acts or  
24 practices that would, or would not, comply with this title.

1 **SEC. 108. NO PRIVATE RIGHT OF ACTION.**

2 This title may not be considered or construed to pro-  
3 vide any private right of action. No private civil action  
4 relating to any act or practice governed under this title  
5 may be commenced or maintained in any State court or  
6 under State law (including a pendent State claim to an  
7 action under Federal law).

8 **SEC. 109. EFFECT ON OTHER LAWS.**

9 (a) **QUALIFIED EXEMPTION FOR COMPLIANCE WITH**  
10 **OTHER FEDERAL PRIVACY LAWS.**—To the extent that  
11 personally identifiable information protected under this  
12 title is also protected under a provision of Federal privacy  
13 law described in subsection (c), a data collection organiza-  
14 tion that complies with the relevant provision of such other  
15 Federal privacy law shall be deemed to have complied with  
16 the corresponding provision of this title.

17 (b) **PROTECTION OF OTHER FEDERAL PRIVACY**  
18 **LAWS.**—Nothing in this title may be construed to modify,  
19 limit, or supersede the operation of the Federal privacy  
20 laws described in subsection (c) or the provision of infor-  
21 mation permitted or required, expressly or by implication,  
22 by such laws, with respect to Federal rights and practices.

23 (c) **OTHER FEDERAL PRIVACY LAWS DESCRIBED.**—  
24 The provisions of law to which subsections (a) and (b)  
25 apply are the following:

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

3           (2) The Right to Financial Privacy Act of 1978  
4 (12 U.S.C. 3401 et seq.).

5           (3) The Fair Credit Reporting Act (15 U.S.C.  
6 1681 et seq.).

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

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

11           (6) Title V of the Gramm-Leach-Bliley Act of  
12 1999 (15 U.S.C. 6801 et seq.).

13           (7) The Electronic Communications Privacy Act  
14 of 1986 (Public Law 99–508).

15           (8) The Driver’s Privacy Protection Act of  
16 1994 (18 U.S.C. 2721 et seq.).

17           (9) The Family Educational Rights and Privacy  
18 Act of 1974 (20 U.S.C. 1221 note, 1232g).

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

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

23           (12) Section 222 of the Communications Act of  
24 1934 (47 U.S.C. 222) relating to the Customer Pro-  
25 prietary Network Information.

1           (13) The Cable Communications Policy Act of  
2           1984 (47 U.S.C. 521 et seq.).

3           (14) The Communications Assistance for Law  
4           Enforcement Act (47 U.S.C. 1001 et seq.).

5           (15) The Video Privacy Protection Act of 1988  
6           (Public Law 100–618).

7           (16) The Telephone Consumer Protection Act  
8           of 1991 (Public Law 102–243).

9           (17) The Health Insurance Portability and Ac-  
10          countability Act of 1996 (Public Law 104–191), as  
11          it relates to an entity described in section 1172(a)  
12          of the Social Security Act (42 U.S.C. 1320d–1(a))  
13          or to activities regulated under section 1173 of such  
14          Act (42 U.S.C. 1320d–2).

15          (d) PREEMPTION OF STATE PRIVACY LAWS.—This  
16          title preempts any statutory law, common law, rule, or  
17          regulation of a State, or a political subdivision of a State,  
18          to the extent such law, rule, or regulation relates to or  
19          affects the collection, use, sale, disclosure, retention, or  
20          dissemination of personally identifiable information in  
21          commerce. No State, or political subdivision of a State,  
22          may take any action to enforce this title.

1 **SEC. 110. EFFECTIVE DATE.**

2 This title shall apply with respect to personally identi-  
3 fiable information collected on or after the date that is  
4 1 year after the date of enactment of this Act.

5 **TITLE II—IDENTITY THEFT**  
6 **PREVENTION AND REMEDIES**

7 **SEC. 201. FACILITATING ELECTRONIC IDENTITY THEFT AF-**  
8 **FIDAVITS.**

9 The Commission shall take such action as necessary  
10 to permit (including by electronic means) consumers that  
11 have a reasonable belief that they are a victim of identity  
12 theft—

13 (1) to enter required consumer information in  
14 the commission-developed document entitled “Iden-  
15 tity Theft Affidavit”; and

16 (2) to submit completed forms and other sup-  
17 plemental information to the Commission and other  
18 entities.

19 **SEC. 202. PROMOTING USE OF COMMON IDENTITY THEFT**  
20 **AFFIDAVIT.**

21 The Commission shall take such action as necessary  
22 to solicit the acceptance and acknowledgement of stand-  
23 ardized Identity Theft Affidavit by entities that receive  
24 disputes regarding the unauthorized use of accounts of  
25 such entities from consumers that have reason to believe  
26 that they are victims of identity theft.

1 **SEC. 203. TIMELY RESOLUTION OF IDENTITY THEFT DIS-**  
2 **PUTES.**

3 The Commission shall require entities that receive  
4 disputes regarding the unauthorized use of accounts of  
5 such entities from consumers that have reason to believe  
6 that they are victims of identity theft to conduct any nec-  
7 essary investigation and decide an outcome of a claim  
8 within 90 days from the date on which all necessary infor-  
9 mation to investigate the claim has been submitted to the  
10 entity.

11 **SEC. 204. IMPROVEMENTS TO CONSUMER CLEARING-**  
12 **HOUSE.**

13 The Commission shall utilize the Identity Theft  
14 Clearinghouse to permit consumers that have a reasonable  
15 belief that they are victims of identity theft to submit any  
16 information relevant to such identity theft to the Clearing-  
17 house (including by means of an Identity Theft Affidavit),  
18 so that such information may be transmitted by the Clear-  
19 ingshouse to appropriate entities for necessary protective  
20 action and to mitigate losses resulting from such identity  
21 theft.

22 **SEC. 205. IMPROVED IDENTITY THEFT DATA.**

23 (a) IN GENERAL.—The Commission shall—

24 (1) establish a process to contact, not less than  
25 annually, public and private entities that receive and  
26 process complaints from consumers that have a rea-

1       sonable belief that they are victims of identity theft;  
2       and

3               (2) obtain accurate data on the incidences and  
4       nature of complaints from such entities.

5       (b) INCLUSION IN DATABASE.—Such information  
6 shall be made part of the Commission’s Identity Theft  
7 Clearinghouse database.

8 **SEC. 206. CHANGE OF ADDRESS PROTECTIONS.**

9       The Commission shall require appropriate entities to  
10 take reasonable steps to verify the accuracy of a con-  
11 sumer’s address, including by confirming a consumer’s  
12 change of address by sending a confirmation of such  
13 change to the old and the new address of the consumer.

14 **SEC. 207. EFFECTIVE DATE.**

15       This title shall take effect 180 days after the date  
16 of enactment of this Act.

17       **TITLE III—INTERNATIONAL**  
18                               **PROVISIONS**

19 **SEC. 301. STUDY BY COMPTROLLER GENERAL.**

20       The Comptroller General of the United States shall  
21 conduct a study and issue a report analyzing the impact  
22 on the interstate and foreign commerce of the United  
23 States of information privacy laws, regulations, or agree-  
24 ments enacted, promulgated, or adopted by other nations,  
25 including regional or international agreements between

1 nations, and whether the enforcement mechanisms or pro-  
2 cedures of those laws, regulations, or agreements result  
3 in discriminatory treatment of United States entities. The  
4 first report under this section shall be issued not later  
5 than 120 days after the date of enactment of this Act and  
6 subsequent reports shall be issued every 3 years there-  
7 after.

8 **SEC. 302. REMEDIATION OF DISCRIMINATORY IMPACT BY**  
9 **SECRETARY OF COMMERCE.**

10 If the Comptroller General of the United States finds,  
11 in the study and report under section 301, that such infor-  
12 mation privacy laws, regulations, or agreements substan-  
13 tially impede interstate and foreign commerce of the  
14 United States and that the enforcement mechanisms or  
15 procedures of the information privacy laws, regulations,  
16 or agreements described in such subsection result in dis-  
17 criminatory treatment of United States entities, the Sec-  
18 retary of Commerce shall, to the extent permitted by law  
19 take all steps necessary to mitigate against such discrimi-  
20 natory impact within 180 days after the report making  
21 such findings is issued.

22 **SEC. 303. EFFECT OF NONREMEDATION.**

23 (a) **RECOMMENDATIONS.**—If by the end of the 180-  
24 day period described in section 302, the Secretary of Com-  
25 merce has not attained complete relief from the discrimi-

1 natory impact described in such subsection, the Secretary  
2 shall report to the Congress and the President rec-  
3 ommendations on action to relieve any such remaining dis-  
4 criminatory impact.

5 (b) FEDERAL AGENCY ACTION AFTER CONSIDER-  
6 ATION BY CONGRESS.—During the period after the Sec-  
7 retary reports recommendations under subsection (a) for  
8 mitigation of discriminatory impact and before the Con-  
9 gress acts with respect to such recommendations, no offi-  
10 cer or employee of any Federal agency may take or con-  
11 tinue any action to enjoin, or impose any penalty on, a  
12 United States entity, or a citizen or legal resident of the  
13 United States, for the purpose of fulfilling an international  
14 obligation of the United States under an international pri-  
15 vacy agreement (other than such an obligation under a  
16 ratified treaty) that resulted in such discriminatory im-  
17 pact.

18 **SEC. 304. HARMONIZATION OF INTERNATIONAL PRIVACY**

19 **LAWS, REGULATIONS, AND AGREEMENTS.**

20 Beginning on the date of enactment of this Act, the  
21 Secretary of Commerce shall provide notice of the provi-  
22 sions of this Act to other nations, individually, or as mem-  
23 bers of international organizations or unions that have en-  
24 acted, promulgated, or adopted information privacy laws,  
25 regulations, or agreements, and shall seek recognition of

1 this Act by such nations, organizations, or unions. The  
2 Secretary shall seek the harmonization of this Act with  
3 such information privacy laws, regulations, or agreements,  
4 to the extent such harmonization is necessary for the ad-  
5 vancement of transnational commerce, including electronic  
6 commerce.

○