

107TH CONGRESS  
2D SESSION

# H. R. 4678

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

---

## IN THE HOUSE OF REPRESENTATIVES

MAY 8, 2002

Mr. STEARNS (for himself, Mr. BOUCHER, Mr. TAUZIN, Mr. TOWNS, Mr. BASS, Mr. BILIRAKIS, Mrs. BONO, Mr. DEAL of Georgia, Ms. ESHOO, Mr. GILLMOR, Mr. GORDON, Mr. GREENWOOD, Mr. KINGSTON, Mr. MORAN of Virginia, Mr. SAWYER, Mr. TERRY, Mr. UPTON, Mr. WALDEN, Mr. WELDON of Florida, Mr. WELLER, and Mr. DAN MILLER of Florida) 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 2002”.

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.

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.

TITLE IV—GENERAL PROVISIONS

- Sec. 401. Definitions.

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:

1           (1) Upon the first instance of collection from  
2           the consumer of personally identifiable information,  
3           that may be used for a purpose unrelated to the  
4           transaction, by a data collection organization, the or-  
5           ganization shall provide the notice at the time per-  
6           sonally identifiable information is collected.

7           (2) Upon a material change in the organiza-  
8           tion’s privacy policy statement under section 102(5),  
9           the organization shall provide the notice, not later  
10          than the first time after such change in policy that  
11          the organization seeks to collect, sell, disclose for  
12          consideration, or use personally identifiable informa-  
13          tion to the extent practicable, to each consumer from  
14          whom the organization has collected such informa-  
15          tion.

16          (b) FORM AND CONTENTS OF NOTICE.—A notice re-  
17          quired under subsection (a) shall be provided in a clear  
18          and concise manner, be prominently displayed or explicitly  
19          stated to the consumer, and contain the following informa-  
20          tion:

21               (1) A statement that the information privacy  
22               practices of the data collection organization raise an  
23               issue of privacy for the consumer that may provide  
24               the consumer with rights under law.

1           (2) A description of the manner in which the  
2           consumer may obtain a privacy policy statement that  
3           meets the requirements of section 102, which may  
4           include providing the consumer with an Internet  
5           website, a hyperlink to such a website, or a toll-free  
6           telephone number from which such a statement may  
7           be obtained.

8           (3) If the notice is required under subsection  
9           (a)(2), a statement that there has been a material  
10          change in the organization's privacy policy.

11 **SEC. 102. PRIVACY POLICY STATEMENTS.**

12          (a) **PRIVACY POLICY.**—A data collection organization  
13 shall establish a privacy policy with respect to the collec-  
14 tion, sale, disclosure for consideration, or use of the per-  
15 sonally identifiable information of consumers, the prin-  
16 cipal elements of which shall be embodied in a privacy pol-  
17 icy statement (or statements) that meets the requirements  
18 of subsection (b).

19          (b) **STATEMENT.**—The statement (or statements) re-  
20 quired under subsection (a) shall meet the following re-  
21 quirements:

22           (1) The statement must be clear and con-  
23 spicuous and written in plain language.

24           (2) The statement must be accessible to all con-  
25 sumers of the data collection organization (regard-

1 less of the means by which a consumer conducts a  
2 transaction with the organization)—

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

4 (B) at the time the data collection organi-  
5 zation first collects personally identifiable infor-  
6 mation about the consumer that may be used  
7 for a purpose unrelated to a transaction with  
8 the consumer and subsequently.

9 (3) With respect to personally identifiable infor-  
10 mation that may be used for a purpose unrelated to  
11 a transaction with the consumer and that is subject  
12 to being collected, sold, disclosed for consideration,  
13 or used under the statement, the statement must  
14 disclose only the following:

15 (A) The identity of each data collection or-  
16 ganization, or a description of each class or  
17 type of data collection organization, that may  
18 collect or use the information.

19 (B) The types of information that may be  
20 collected, sold, disclosed for consideration, or  
21 used.

22 (C) How the information may be used.

23 (D) Whether the consumer is required to  
24 provide the information in order to do business  
25 with the data collection organization.

1           (E) The extent to which the information is  
2           subject to sale or disclosure for consideration to  
3           a data collection organization that is not an in-  
4           formation-sharing affiliate of the data collection  
5           organization providing the statement, including  
6           the following:

7                   (i) A clear and prominent statement  
8                   of the fact that the information is subject  
9                   to such sale or disclosure for consideration.

10                   (ii) A description of each class or type  
11                   of data collection organization to which the  
12                   information may be sold or disclosed for  
13                   consideration.

14                   (iii) The purpose for which the infor-  
15                   mation may be used.

16           (F) Whether the information security prac-  
17           tices of the data collection organization meet  
18           the security requirements of section 105 in  
19           order to prevent unauthorized disclosure or re-  
20           lease of personally identifiable information.

21           (c) COMMISSION FACILITATION.—The Commission  
22           shall take actions (including conducting industry-wide  
23           workshops) to facilitate the development of harmonized,  
24           universal wording or logo-based graphics in order to con-

1 vey the contents of privacy policy statements required  
2 under this section.

3 **SEC. 103. CONSUMER OPPORTUNITY TO LIMIT SALE OR DIS-**  
4 **CLOSURE OF INFORMATION.**

5 (a) PRECLUSION OF SALE OR DISCLOSURE.—

6 (1) REQUIREMENT.—A data collection organi-  
7 zation shall provide to the consumer, without charge,  
8 the opportunity to preclude any sale or disclosure for  
9 consideration of the consumer’s personally identifi-  
10 able information, that may be used for a purpose  
11 unrelated to a transaction with the consumer, to any  
12 data collection organization that is not an informa-  
13 tion-sharing partner of the data collection organiza-  
14 tion providing such opportunity.

15 (2) DURATION.—A preclusion on sale or disclo-  
16 sure for consideration of information established by  
17 a consumer under this subsection shall remain in ef-  
18 fect for 5 years or until the consumer indicates oth-  
19 erwise, whichever occurs sooner. A data collection  
20 organization may not seek reconsideration of a con-  
21 sumer’s preclusion of such sale or disclosure until at  
22 least 1 year after such preclusion has been imposed  
23 by the consumer.

24 (b) PERMISSION FOR SALE OR DISCLOSURE.—A data  
25 collection organization may provide the consumer an op-

1 opportunity to permit the sale or disclosure described in sub-  
2 section (a)(1) in exchange for a benefit to the consumer.

3 (c) ACCESSIBILITY.—The opportunity to preclude (or  
4 if offered, to permit) the sale or disclosure for consider-  
5 ation of information under this section must be both easy  
6 to access and use.

7 **SEC. 104. CONSUMER OPPORTUNITY TO LIMIT OTHER IN-**  
8 **FORMATION PRACTICES.**

9 If a data collection organization provides to a con-  
10 sumer the opportunity to limit other practices of the data  
11 collection organization with respect to collection or use of  
12 personally identifiable information regarding the con-  
13 sumer, other than that required by section 103—

14 (1) that opportunity must be easy to access and  
15 to use; and

16 (2) any limitation exercised by the consumer  
17 pursuant to the opportunity shall remain in effect,  
18 unless—

19 (A) the limitation is withdrawn by the con-  
20 sumer; or

21 (B) the data collection organization pro-  
22 vides the consumer at least 30 days notice be-  
23 fore terminating its compliance with the limita-  
24 tion.



1 **SEC. 105. INFORMATION SECURITY OBLIGATIONS.**

2 (a) INFORMATION SECURITY POLICY.—

3 (1) IMPLEMENTATION.—A data collection orga-  
4 nization shall prepare, revise as necessary, and im-  
5 plement an information security policy that is appli-  
6 cable to the information security practices and treat-  
7 ment of personally identifiable information main-  
8 tained by the data collection organization, in order  
9 to prevent the unauthorized disclosure or release of  
10 such information.

11 (2) MANAGEMENT APPROVAL.—An information  
12 security policy created pursuant to paragraph (1)  
13 shall be considered and approved by the senior man-  
14 agement officials of the data collection organization.

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

17 (A) a process for taking corrective action  
18 pursuant to subsection (b); and

19 (B) identifying an officer of the data col-  
20 lection organization as the point of contact with  
21 responsibility for information security issues for  
22 the organization.

23 (b) CORRECTIVE ACTIONS.—

24 (1) NOTIFICATION AND ACTION.—Except as  
25 provided in paragraph (2), upon the joint issuance  
26 of an information security notification by a Federal

1 Government agency and the CERT Coordination  
2 Center, a data collection organization shall take ap-  
3 propriate action, within a reasonable period of time  
4 after being informed and pursuant to its information  
5 security policy, to implement any necessary changes  
6 to its security practices and the architecture, instal-  
7 lation, or implementation of its network or operating  
8 software (including corrective patches) in response  
9 to such a notification.

10 (2) EXCEPTIONS.—A data collection organiza-  
11 tion shall not be required to take the action specified  
12 in a notification under paragraph (1) if—

13 (A) the corrective action required would  
14 cause harm to, or weaken, the organization’s  
15 existing information security for personally  
16 identifiable information or the procedures or  
17 systems of the organization;

18 (B) the organization takes, or has taken,  
19 other appropriate steps or corrective action to  
20 mitigate the vulnerabilities and exposure risks  
21 identified in the notification; or

22 (C) the specified corrective action is not  
23 necessary.

24 (3) CERT COORDINATION CENTER DE-  
25 SCRIBED.—For purposes of this section, the CERT

1 Coordination Center is the Computer Emergency  
2 Response Team Coordination Center of the Software  
3 Engineering Institute operated by Carnegie Mellon  
4 University in Pittsburgh, Pennsylvania, or if such  
5 center is unavailable, an equivalent center des-  
6 ignated by the Commission.

7 (c) EFFECT OF RELEASE OF PERSONALLY IDENTIFI-  
8 ABLE INFORMATION.—If the security of a data collection  
9 organization has been compromised, resulting in the unau-  
10 thorized release of a consumer’s personally identifiable in-  
11 formation, the Commission shall treat the failure of the  
12 data collection organization to comply with its own secu-  
13 rity policy or respond to a Federal agency information se-  
14 curity notification in accordance with subsection (b)(1) as  
15 one factor in determining whether that data collection or-  
16 ganization has violated this section.

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

18 (a) SELF-REGULATORY PROGRAM.—

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

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

1 (B) complies with the guidelines, proce-  
2 dures, requirements, and restrictions of the pro-  
3 gram (including a remedial process under sub-  
4 section (c)(7)).

5 (2) EFFECT OF WILLFUL NONCOMPLIANCE.—A  
6 data collection organization that participates in a  
7 self-regulatory program under this section shall not  
8 be liable for a civil penalty arising out of a violation  
9 of any provision of sections 101 through 105 unless  
10 such violation results from willful noncompliance  
11 with the guidelines, procedures, requirements, or re-  
12 strictions of the program.

13 (b) APPROVAL BY COMMISSION.—

14 (1) APPROVAL.—The Commission shall, within  
15 90 days after submission of an application for ap-  
16 proval of a self-regulatory program under this sec-  
17 tion (or of a material change in a program pre-  
18 viously approved by the Commission), approve such  
19 program (or change) if the Commission finds that  
20 the program (or change) complies with the require-  
21 ments of subsection (c).

22 (2) FORM OF APPLICATION.—The Commission  
23 shall accept an application for approval under para-  
24 graph (1) in any reasonable form the applicant may  
25 submit.

1           (3) DURATION UNTIL RENEWAL.—A self-regu-  
2           latory program approved by the Commission under  
3           paragraph (1) shall be approved for a period of 8  
4           years.

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

10          (c) REQUIREMENTS OF SELF-REGULATORY PRO-  
11          GRAM.—A self-regulatory program complies with the re-  
12          quirements of this subsection if the program provides each  
13          of the following:

14                (1) Guidelines and procedures requiring a pro-  
15                gram participant to provide equivalent or greater  
16                protections for consumers and their personally iden-  
17                tifiable information as are provided under sections  
18                101 through 105.

19                (2) Procedures and requirements to provide  
20                for—

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

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

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

12 (D) random compliance testing of partici-  
13 pants, and compliance testing of participants  
14 with a high number of complaints against them,  
15 to determine the tested participant's compliance  
16 with the program; and

17 (E) regular compliance testing of a partici-  
18 pant, which shall take place not less frequently  
19 than every 4 years, with respect to the privacy  
20 policy and practices of the participant, to en-  
21 sure that the self-reviews and self-certifications  
22 of the participant are accurate and comply with  
23 the program.

24 (3) Procedures and requirements that ensure  
25 that a program participant provides a process for re-

1 solving disputes with consumers relating to the pri-  
2 vacy policy and practices of the participant. Such  
3 dispute resolution process—

4 (A) must be available without charge to a  
5 consumer;

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

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

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

14 (E)

15 (i) must be completed within 30 days  
16 after submission of the dispute by the con-  
17 sumer; or

18 (ii) must be completed within 60 days  
19 after submission of the dispute by the con-  
20 sumer, if the participant—

21 (I) determines that additional  
22 time is required to obtain information  
23 to make an informed decision with re-  
24 spect to the dispute; and

1 (II) notifies the consumer that  
2 such additional time is required.

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

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

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

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

19 (6) Requirements and restrictions that assure  
20 independence with respect to program eligibility,  
21 compliance, and dispute resolution mechanisms and  
22 decisions from improper interference by management  
23 or ownership of the self-regulatory program partici-  
24 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, the con-  
9 sumer shall initially seek resolution through the par-  
10 ticipant’s dispute resolution process (established in  
11 accordance with subsection (c)(3)). The Commission  
12 shall promptly refer to the participant involved any  
13 dispute submitted to the Commission for which reso-  
14 lution has not been initially sought through such  
15 process.

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

21                   (A) The dispute was initially submitted  
22                   under paragraph (1) for resolution through the  
23                   participant’s dispute resolution process.

24                   (B) The dispute submitted under para-  
25                   graph (1) is not resolved—

1 (i) within 30 days after submission of  
2 the dispute by the consumer; or

3 (ii) to the satisfaction of the con-  
4 sumer.

5 (C) Notice of the facts of the dispute is  
6 submitted to the Commission not later than 30  
7 days after the date on which the consumer is  
8 notified of the resolution through the partici-  
9 pant's dispute resolution process.

10 (D) The consumer has not voluntarily ac-  
11 cepted a resolution of the dispute under para-  
12 graph (1).

13 (E) The dispute was not resolved through  
14 binding arbitration.

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

23 (f) MISREPRESENTATION OF SELF-REGULATORY  
24 PROGRAM PARTICIPATION.—It is unlawful for a data col-  
25 lection organization to misrepresent that it is a participant

1 in a self-regulatory program (including through any mech-  
2 anism provided under subsection (c)(4)) when such orga-  
3 nization is not, in fact, such a participant.

4 (g) EXEMPTED ENTITY PARTICIPATION.—An entity  
5 that is not a data collection organization and that volun-  
6 tarily participates in a self-regulatory program under this  
7 section shall enjoy the rights and benefits provided under  
8 this section.

9 **SEC. 107. ENFORCEMENT.**

10 (a) UNFAIR OR DECEPTIVE ACT OR PRACTICE.—A  
11 violation of any provision of this title is an unfair or decep-  
12 tive act or practice unlawful under section 5(a)(1) of the  
13 Federal Trade Commission Act (15 U.S.C. 45(a)(1)), ex-  
14 cept that the amount of any civil penalty under such Act  
15 shall be doubled for a violation of this title, but may not  
16 exceed \$500,000 for all related violations by a single viola-  
17 tor (without respect to the number of consumers affected  
18 or the duration of 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 issue generally applicable guidelines and, upon  
22 request, advisory opinions with respect specific types of  
23 acts or practices that would, or would not, comply with  
24 this title, but may not prescribe regulations to carry out  
25 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, or dissemina-  
20          tion of personally identifiable information in commerce.  
21          No State, or political subdivision of a State, may take any  
22          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 a victim 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 a victim 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 victim 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 inghouse 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 a victim 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 subsection (a), that such  
12 information privacy laws, regulations, or agreements sub-  
13 stantially 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 (b) 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.

## 7 **TITLE IV—GENERAL** 8 **PROVISIONS**

### 9 **SEC. 401. DEFINITIONS.**

10 In this Act:

11 (1) The term “Commission” means the Federal  
12 Trade Commission.

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

16 (3)(A) The term “data collection organization”  
17 means an entity (or an agent or affiliate of the enti-  
18 ty) that collects (by any means, through any me-  
19 dium), sells, discloses for consideration, or uses per-  
20 sonally identifiable information of the consumer.

21 (B) Such term does not include—

22 (i) a governmental agency; or

23 (ii) a not-for-profit entity, to the extent  
24 that personally identifiable information is not  
25 used for a commercial purpose; or

1 (iii) an entity that—

2 (I) has annual gross revenue under  
3 \$1,000,000 (based on the value of such  
4 amount in fiscal year 2000, adjusted for  
5 current dollars);

6 (II) has fewer than 25 employees;

7 (III) collects or uses personally identi-  
8 fiable information from fewer than 1,000  
9 consumers for a purpose unrelated to a  
10 transaction with the consumer;

11 (IV) does not process personally iden-  
12 tifiable information of consumers; and

13 (V) does not sell or disclose for con-  
14 sideration such information to another per-  
15 son.

16 (4)(A) The term “personally identifiable infor-  
17 mation”, with respect to a data collection organiza-  
18 tion means individually identifiable information re-  
19 lating to a living individual who can be identified  
20 from that information.

21 (B) Such term includes—

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

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

- 1 (iii) electronic mail address;  
2 (iv) telephone number;  
3 (v) social security number; or  
4 (vi) any other unique identifying informa-  
5 tion that a data collector and processor collects  
6 and combines with any information described in  
7 the preceding subparagraphs of this paragraph.

8 (C) Such term does not include—

9 (i) anonymous or aggregate data, or any  
10 other information that does not identify a  
11 unique living individual;

12 (ii) information about a consumer inferred  
13 from data maintained about a consumer; or

14 (iii) information about a consumer ob-  
15 tained from a public record.

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

19 (6) The term “information-sharing partner”  
20 means, with respect to a data collection organiza-  
21 tion, an entity that is contractually obligated to com-  
22 ply with the practices enumerated under the privacy  
23 policy statement of the organization required under  
24 section 102.

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

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

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

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

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

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

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

1           (D) any use of information to evaluate, de-  
2           tect, or reduce the risk of fraud or other crimi-  
3           nal activity, or other risk-management activi-  
4           ties.

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

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

14          (11) The term “purchase” means providing, di-  
15          rectly or indirectly, anything of value in exchange  
16          for a benefit.

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

○