

106TH CONGRESS
2D SESSION

S. 2606

To protect the privacy of American consumers.

IN THE SENATE OF THE UNITED STATES

MAY 23, 2000

Mr. HOLLINGS (for himself, Mr. ROCKEFELLER, Mr. BRYAN, Mr. BREAUX, Mr. INOUE, Mr. FEINGOLD, Mr. EDWARDS, Mr. KERREY, Mr. CLELAND, Mr. DURBIN, and Mr. BYRD) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To protect the privacy of American consumers.

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”.

6 **SEC. 2. FINDINGS.**

7 The Congress makes the following findings:

8 (1) The right to privacy is a personal and fun-
9 damental right worthy of protection through appro-
10 prium legislation.

1 (2) Consumers engaging in and interacting with
2 companies engaged in interstate commerce have an
3 ownership interest in their personal information, as
4 well as a right to control how that information is
5 collected, used, or transferred.

6 (3) Existing State, local, and Federal laws pro-
7 vide virtually no privacy protection for Internet
8 users.

9 (4) Moreover, existing privacy regulation of the
10 general, or offline, marketplace provides inadequate
11 consumer protections in light of the significant data
12 collection and dissemination practices employed
13 today.

14 (5) The Federal Government thus far has es-
15 chewed general Internet privacy laws in favor of in-
16 dustry self-regulation, which has led to several self-
17 policing schemes, none of which are enforceable in
18 any meaningful way or provide sufficient consumer
19 protection.

20 (6) State governments have been reluctant to
21 enter the field of Internet privacy regulation because
22 use of the Internet often crosses State, or even na-
23 tional, boundaries.

24 (7) States are nonetheless interested in pro-
25 viding greater privacy protection to their citizens as

1 evidenced by recent lawsuits brought against offline
2 and online companies by State attorneys general to
3 protect consumer privacy.

4 (8) Personal information flowing over the Inter-
5 net requires greater privacy protection than is cur-
6 rently available today. Vast amounts of personal in-
7 formation about individual Internet users are col-
8 lected on the Internet and sold or otherwise trans-
9 ferred to third parties.

10 (9) Poll after poll consistently demonstrates
11 that individual Internet users are highly troubled
12 over their lack of control over their personal infor-
13 mation.

14 (10) Research on the Internet industry dem-
15 onstrates that consumer concerns about their pri-
16 vacy on the Internet has a correlative negative im-
17 pact on the development of e-commerce.

18 (11) Notwithstanding these concerns, the Inter-
19 net is becoming a major part of the personal and
20 commercial lives of millions of Americans, providing
21 increased access to information, as well as commu-
22 nications and commercial opportunities.

23 (12) It is important to establish personal pri-
24 vacy rights and industry obligations now so that
25 consumers have confidence that their personal pri-

1 vacy is fully protected on our Nation’s telecommuni-
2 cations networks and on the Internet.

3 (13) The social and economic costs of imposing
4 obligations on industry now will be lower than if
5 Congress waits until the Internet becomes more
6 prevalent in our everyday lives in coming years.

7 (14) Absent the recognition of these rights and
8 the establishment of consequent industry responsibil-
9 ities to safeguard those rights, consumer privacy will
10 soon be more gravely threatened.

11 (15) The ease of gathering and compiling per-
12 sonal information on the Internet, both overtly and
13 surreptitiously, is becoming increasingly efficient
14 and effortless due to advances in digital communica-
15 tions technology which have provided information
16 gatherers the ability to seamlessly compile highly de-
17 tailed personal histories of Internet users.

18 (16) Consumers must have—

19 (A) clear and conspicuous notice that in-
20 formation is being collected about them;

21 (B) clear and conspicuous notice as to the
22 information gatherer’s intent with respect to
23 that information;

24 (C) the ability to control the extent to
25 which information is collected about them; and

1 (D) the right to prohibit any unauthorized
2 use, reuse, disclosure, transfer, or sale of their
3 information.

4 (17) Fair information practices include pro-
5 viding consumers with knowledge of any data collec-
6 tion clear and conspicuous notice of an entity's in-
7 formation practices, the ability to control whether or
8 not those practices will be applied to them person-
9 ally, access to information collected about them, and
10 safeguards to ensure the integrity and security of
11 that information.

12 (18) Recent surveys of websites conducted by
13 the Federal Trade Commission and Georgetown Uni-
14 versity found that a small minority of websites sur-
15 veyed contained a privacy policy embodying fair in-
16 formation practices such as notice, choice, access,
17 and security.

18 (19) Americans expect that their purchases of
19 written materials, videos, and music will remain con-
20 fidential, whether they are shopping online or in the
21 traditional workplace.

22 (20) Consumer privacy with respect to written
23 materials, music, and movies should be protected
24 vigilantly to ensure the free exercise of First Amend-
25 ment rights of expression, regardless of medium.

1 (21) Under current law, millions of American
2 cable customers are protected against disclosures of
3 their personal subscriber information without notice
4 and choice, whereas no similar protection is available
5 to subscribers of multichannel video programming
6 via satellite.

7 (22) Almost every American is a consumer of
8 some form of communications service, be it wireless,
9 wireline, cable, broadcast, or satellite.

10 (23) In light of the convergence of and emerg-
11 ing competition among and between wireless,
12 wireline, satellite, broadcast, and cable companies,
13 privacy safeguards should be applied uniformly
14 across different communications media so as to pro-
15 vide consistent consumer privacy protections as well
16 as a level competitive playing field for industry.

17 (24) Notwithstanding the recent focus on Inter-
18 net privacy, privacy issues abound in the traditional,
19 or offline, marketplace that merit Federal attention.

20 (25) The Congress would benefit from an ex-
21 haustive analysis of general marketplace privacy
22 issues conducted by the agency with the most exper-
23 tise in this area, the Federal Trade Commission.

24 (26) While American workers are growing in-
25 creasingly concerned that their employers may be

1 violating their privacy, many workers are unaware
2 that their activities in the workplace may be subject
3 to significant and potentially invasive monitoring.

4 (27) While employers may have a legitimate
5 need to maintain an efficient and productive work-
6 force, that need should not improperly impinge on
7 employee privacy rights in the workplace.

8 (28) Databases containing personal information
9 about consumers' commercial purchasing, browsing,
10 and shopping habits, as well as their generalized
11 product preferences, represent considerable commer-
12 cial value.

13 (29) These databases should not be considered
14 an asset with respect to creditors' interests if the
15 asset holder has availed itself of the protection of
16 State or Federal bankruptcy laws.

17 **SEC. 3. PREEMPTION OF INCONSISTENT STATE LAW OR**
18 **REGULATIONS.**

19 (a) IN GENERAL.—Except as provided in subsection
20 (b), this Act preempts any State law, regulation, or rule
21 that is inconsistent with the provisions of this Act.

22 (b) EXCEPTIONS.—

23 (1) IN GENERAL.—Nothing in this Act
24 preempts—

25 (A) the law of torts in any State;

1 (B) the common law in any State; or

2 (C) any State law, regulation, or rule that
3 prohibits fraud or provides a remedy for fraud.

4 (2) PRIVATE RIGHT-OF-ACTION.—Notwith-
5 standing subsection (a), if a State law provides for
6 a private right-of-action under a statute enacted to
7 provide consumer protection, nothing in this Act
8 precludes a person from bringing such an action
9 under that statute, even if the statute is otherwise
10 preempted in whole or in part under subsection (a).

11 **SEC. 4. TABLE OF CONTENTS.**

12 The table of contents of this Act is as follows:

Sec. 1. Short title.

Sec. 2. Findings.

Sec. 3. Preemption of inconsistent State law or regulations.

Sec. 4. Table of contents.

TITLE I—ONLINE PRIVACY

Sec. 101. Collection or disclosure of personally identifiable information.

Sec. 102. Notice, consent, access, and security requirements.

Sec. 103. Other kinds of information.

Sec. 104. Exceptions.

Sec. 105. Permanence of consent.

Sec. 106. Disclosure to law enforcement agency or under court order.

Sec. 107. Effective date.

Sec. 108. FTC rulemaking procedure required.

TITLE II—PRIVACY PROTECTION FOR CONSUMERS OF
BOOKS, RECORDED MUSIC, AND VIDEOS

Sec. 201. Extension of video rental protections to books and recorded music.

Sec. 202. Effective Date.

TITLE III—ENFORCEMENT AND REMEDIES

Sec. 301. Enforcement.

Sec. 302. Violation is unfair or deceptive act or practice.

Sec. 303. Private right of action.

Sec. 304. Actions by States.

Sec. 305. Whistleblower protection.

Sec. 306. No effect on other remedies.

Sec. 307. FTC Office of Online Privacy.

TITLE IV—COMMUNICATIONS TECHNOLOGY PRIVACY
PROTECTIONS

Sec. 401. Privacy protection for subscribers of satellite television services for private home viewing.

Sec. 402. Customer proprietary network information.

TITLE V—RULEMAKING AND STUDIES

Sec. 501. Federal Trade Commission examination.

Sec. 502. Federal Communications Commission rulemaking.

Sec. 503. Department of Labor study of privacy issues in the workplace.

TITLE VI—PROTECTION OF PERSONALLY IDENTIFI-
ABLE INFORMATION IN BANKRUPTCY

Sec. 601. Personally identifiable information not asset in bankruptcy.

TITLE VII—INTERNET SECURITY INITIATIVES

Sec. 701. Findings.

Sec. 702. Computer Security Partnership Council.

Sec. 703. Research and development.

Sec. 704. Computer security training programs.

Sec. 705. Government information security standards.

Sec. 706. Recognition of quality in computer security practices.

Sec. 707. Development of automated privacy controls.

TITLE VIII—CONGRESSIONAL INFORMATION SECURITY
STANDARDS

Sec. 801. Exercise of rulemaking power.

Sec. 802. Senate.

TITLE IX—DEFINITIONS

Sec. 901. Definitions.

1 **TITLE I—ONLINE PRIVACY**

2 **SEC. 101. COLLECTION OR DISCLOSURE OF PERSONALLY**
3 **IDENTIFIABLE INFORMATION.**

4 An Internet service provider, online service provider,
5 or operator of a commercial website on the Internet may
6 not collect, use, or disclose personally identifiable informa-
7 tion about a user of that service or website except in ac-
8 cordance with the provisions of this title.

9 **SEC. 102. NOTICE, CONSENT, ACCESS, AND SECURITY RE-**
10 **QUIREMENTS.**

11 (a) NOTICE.—An Internet service provider, online
12 service provider, or operator of a commercial website may
13 not collect personally identifiable information from a user
14 of that service or website unless that provider or operator
15 gives clear and conspicuous notice in a manner reasonably

1 calculated to provide actual notice to any user or prospec-
2 tive user that personally identifiable information may be
3 collected from that user. The notice shall disclose—

4 (1) the specific information that will be col-
5 lected;

6 (2) the methods of collecting and using the in-
7 formation collected; and

8 (3) all disclosure practices of that provider or
9 operator for personally identifiable information so
10 collected, including whether it will be disclosed to
11 third parties.

12 (b) CONSENT.—An Internet service provider, online
13 service provider, or operator of a commercial website may
14 not—

15 (1) collect personally identifiable information
16 from a user of that service or website, or

17 (2) except as provided in section 107, disclose
18 or otherwise use such information about a user of
19 that service or website,

20 unless the provider or operator obtains that user's affirm-
21 ative consent, in advance, to the collection and disclosure
22 or use of that information.

23 (c) ACCESS.—An Internet service provider, online
24 service provider, or operator of a commercial website
25 shall—

1 (1) upon request provide reasonable access to a
2 user to personally identifiable information that the
3 provider or operator has collected after the effective
4 date of this title relating to that user;

5 (2) provide a reasonable opportunity for a user
6 to correct, delete, or supplement any such informa-
7 tion maintained by that provider or operator; and

8 (3) make the correction or supplementary infor-
9 mation a part of that user's personally identifiable
10 information for all future disclosure and other use
11 purposes.

12 (d) SECURITY.—An Internet service provider, online
13 service provider, or operator of a commercial website shall
14 establish and maintain reasonable procedures necessary to
15 protect the security, confidentiality, and integrity of per-
16 sonally identifiable information maintained by that pro-
17 vider or operator.

18 (e) NOTICE OF POLICY CHANGE.—Whenever an
19 Internet service provider, online service provider, or oper-
20 ator of a commercial website makes a material change in
21 its policy for the collection, use, or disclosure of personally
22 identifiable information, it—

23 (1) shall notify all users of that service or
24 website of the change in policy; and

1 (2) may not collect, disclose, or otherwise use
2 any personally identifiable information in accordance
3 with the changed policy unless the user has affirma-
4 tively consented, under subsection (b), to its collec-
5 tion, disclosure, or use in accordance with the
6 changed policy.

7 (f) NOTICE OF PRIVACY BREACH.—

8 (1) IN GENERAL.—If an Internet service pro-
9 vider, online service provider, or operator of a com-
10 mercial website commits a breach of privacy with re-
11 spect to the personally identifiable information of a
12 user, then it shall, as soon as reasonably possible,
13 notify all users whose personally identifiable infor-
14 mation was affected by that breach. The notice shall
15 describe the nature of the breach and the steps
16 taken by the provider or operator to remedy it.

17 (2) BREACH OF PRIVACY.—For purposes of
18 paragraph (1), an Internet service provider, online
19 service provider, or operator of a commercial website
20 commits a breach of privacy with respect to person-
21 ally identifiable information of a user if—

22 (A) it collects, discloses, or otherwise uses
23 personally identifiable information in violation
24 of any provision of this title; or

1 (B) it knows that the security, confiden-
2 tiality, or integrity of personally identifiable in-
3 formation is compromised by any act or failure
4 to act on the part of the provider or operator
5 or by any function of the Internet service or on-
6 line service provided, or commercial website op-
7 erated, by that provider or operator that re-
8 sulted in a disclosure, or possible disclosure, of
9 that information.

10 (g) APPLICATION TO CERTAIN THIRD-PARTY OPERA-
11 TORS.—The provisions of this section applicable to Inter-
12 net service providers, online service providers, and com-
13 mercial website operators apply to any third party, includ-
14 ing an advertiser, that uses that service or website to col-
15 lect information about users of that service or website.

16 **SEC. 103. OTHER KINDS OF INFORMATION.**

17 (a) IN GENERAL.—Except as provided in subsection
18 (b), the provisions of sections 101 and 102 (except for
19 subsections (b), (c), and (e)(2)) that apply to personally
20 identifiable information apply also to the collection and
21 disclosure or other use of information about users of an
22 Internet service, online service, or commercial website that
23 is not personally identifiable information.

1 (b) CONSENT RULE.—An Internet service provider,
2 online service provider, or operator of a commercial
3 website may not—

4 (1) collect information described in subsection

5 (a) from a user of that service or website, or

6 (2) except as provided in section 107, disclose
7 or otherwise use such information about a user of
8 that service or website,

9 unless the provider or operator obtains that user's consent
10 to the collection and disclosure or other use of that infor-
11 mation. For purposes of this subsection, the user will be
12 deemed to have consented unless the user objects to the
13 collection and disclosure or other use of the information.

14 (c) APPLICATION TO CERTAIN THIRD-PARTY OPERA-
15 TORS.—The provisions of this section applicable to Inter-
16 net service providers, online service providers, and com-
17 mercial website operators apply to any third party, includ-
18 ing an advertiser, that uses that service or website to col-
19 lect information about users of that service or website.

20 **SEC. 104. EXCEPTIONS.**

21 (a) IN GENERAL.—Sections 102 and 103 do not
22 apply to the collection, disclosure, or use by an Internet
23 service provider, online service provider, or operator of a
24 commercial website of information about a user of that
25 service or website—

1 (1) to protect the security or integrity of the
2 service or website; or

3 (2) to conduct a transaction, deliver a product
4 or service, or complete an arrangement for which the
5 user provided the information.

6 (b) DISCLOSURE TO PARENT PROTECTED.—An
7 Internet service provider, online service provider, or oper-
8 ator of a commercial website may not be held liable under
9 this title, any other Federal law, or any State law for any
10 disclosure made in good faith and following reasonable
11 procedures in responding to a request for disclosure of
12 personal information under section 1302(b)(1)(B)(iii) of
13 the Children’s Online Privacy Protection Act of 1998 to
14 the parent of a child.

15 **SEC. 105. PERMANENCE OF CONSENT.**

16 The consent or denial of consent by a user of permis-
17 sion to an Internet service provider, online service pro-
18 vider, or operator of a commercial website to collect, dis-
19 close, or otherwise use any information about that user
20 for which consent is required under this title—

21 (1) shall remain in effect until changed by the
22 user;

23 (2) except as provided in section 102(e), shall
24 apply to any revised, modified, new, or improved

1 service provided by that provider or operator to that
2 user; and

3 (3) except as provided in section 102(e), shall
4 apply to the collection, disclosure, or other use of
5 that information by any entity that is a commercial
6 successor of that provider or operator, without re-
7 gard to the legal form in which such succession was
8 accomplished.

9 **SEC. 106. DISCLOSURE TO LAW ENFORCEMENT AGENCY OR**
10 **UNDER COURT ORDER.**

11 (a) IN GENERAL.—Notwithstanding any other provi-
12 sion of this title, an Internet service provider, online serv-
13 ice provider, operator of a commercial website, or third
14 party that uses such a service or website to collect infor-
15 mation about users of that service or website may disclose
16 personally identifiable information about a user of that
17 service or website—

18 (1) to a law enforcement agency in response to
19 a warrant issued under the Federal Rules of Crimi-
20 nal Procedure, an equivalent State warrant, or a
21 court order issued in accordance with subsection (c);
22 and

23 (2) in response to a court order in a civil pro-
24 ceeding granted upon a showing of compelling need

1 for the information that cannot be accommodated by
2 any other means if—

3 (A) the user to whom the information re-
4 lates is given reasonable notice by the person
5 seeking the information of the court proceeding
6 at which the order is requested; and

7 (B) that user is afforded a reasonable op-
8 portunity to appear and contest the issuance of
9 requested order or to narrow its scope.

10 (b) SAFEGUARDS AGAINST FURTHER DISCLO-
11 SURE.—A court that issues an order described in sub-
12 section (a) shall impose appropriate safeguards on the use
13 of the information to protect against its unauthorized dis-
14 closure.

15 (c) COURT ORDERS.—A court order authorizing dis-
16 closure under subsection (a)(1) may issue only with prior
17 notice to the user and only if the law enforcement agency
18 shows that there is probable cause to believe that the user
19 has engaged, is engaging, or is about to engage in criminal
20 activity and that the records or other information sought
21 are material to the investigation of such activity. In the
22 case of a State government authority, such a court order
23 shall not issue if prohibited by the law of such State. A
24 court issuing an order pursuant to this subsection, on a
25 motion made promptly by the Internet service provider,

1 online service provider, or operator of the commercial
2 website, may quash or modify such order if the informa-
3 tion or records requested are unreasonably voluminous in
4 nature or if compliance with such order otherwise would
5 cause an unreasonable burden on the provider or operator.

6 **SEC. 107. EFFECTIVE DATE.**

7 (a) IN GENERAL.—This title takes effect after the
8 Federal Trade Commission completes the rulemaking pro-
9 cedure under section 109.

10 (b) APPLICATION TO PRE-EXISTING DATA.—

11 (1) IN GENERAL.—After the effective date of
12 this title, and except as provided in paragraphs (2)
13 and (3), sections 101, 102, and 103 apply to infor-
14 mation collected before the date of enactment of this
15 Act.

16 (2) COLLECTION OF BOTH KINDS OF INFORMA-
17 TION.—Section 102(b)(1) and 103(b)(1) do not
18 apply to information collected before the effective
19 date of this title.

20 (3) ACCESS TO PERSONALLY IDENTIFIABLE IN-
21 FORMATION.—Section 102(c) applies to personally
22 identifiable information collected before the effective
23 date of this title unless it is economically unfeasible
24 for the Internet service provider, online service pro-

1 vider, or commercial website operator to comply with
 2 that section for the information.

3 **SEC. 108. FTC RULEMAKING PROCEDURE REQUIRED.**

4 The Federal Trade Commission shall initiate a rule-
 5 making procedure within 90 days after the date of enact-
 6 ment of this Act to implement the provisions of this title.
 7 Notwithstanding any requirement of chapter 5 of title 5,
 8 United States Code, the Commission shall complete the
 9 rulemaking procedure not later than 270 days after it is
 10 commenced.

11 **TITLE II—PRIVACY PROTECTION**
 12 **FOR CONSUMERS OF BOOKS,**
 13 **RECORDED MUSIC, AND VID-**
 14 **EOS**

15 **SEC. 201. EXTENSION OF VIDEO RENTAL PROTECTIONS TO**
 16 **BOOKS AND RECORDED MUSIC.**

17 (a) IN GENERAL.—Section 2710 of title 18, United
 18 States Code, is amended by striking the section designa-
 19 tion and all that follows through the end of subsection (b)
 20 and inserting the following:

21 **“§ 2710. Wrongful disclosure of information about**
 22 **video, book, or recorded music rental,**
 23 **sale, or delivery**

24 **“(a) DEFINITIONS.—In this section:**

1 “(1) The term ‘book dealer’ means any person
2 engaged in the business, in or affecting interstate or
3 foreign commerce, of renting, selling, or delivering
4 books, magazines, or other written or printed mate-
5 rial (regardless of the format or medium), or any
6 person or other entity to whom a disclosure is made
7 under subparagraph (D) or (E) of subsection (b)(2),
8 but only with respect to the information contained in
9 the disclosure.

10 “(2) The term ‘recorded music dealer’ means
11 any person, engaged in the business, in or affecting
12 interstate or foreign commerce, of selling, renting, or
13 delivering recorded music, regardless of the format
14 in which or medium on which it is recorded, or any
15 person or other entity to whom a disclosure is made
16 under subparagraph (D) or (E) of subsection (b)(2),
17 but only with respect to the information contained in
18 the disclosure.

19 “(3) The term ‘consumer’ means any renter,
20 purchaser, or user of goods or services from a video
21 provider, book dealer, or recorded music dealer.

22 “(4) The term ‘ordinary course of business’
23 means only debt-collection activities, order fulfill-
24 ment, request processing, and the transfer of owner-
25 ship.

1 “(5) The term ‘personally identifiable informa-
2 tion’ means information that identifies a person as
3 having requested or obtained specific video materials
4 or services, specific books, magazines, or other writ-
5 ten or printed materials, or specific recorded music.

6 “(6) The term ‘video provider’ means any per-
7 son engaged in the business, in or affecting inter-
8 state or foreign commerce, of rental, sale, or delivery
9 of recorded videos, regardless of the format in
10 which, or medium on which they are recorded, or
11 similar audio-visual materials, or any person or
12 other entity to whom a disclosure is made under
13 subparagraph (D) or (E) of subsection (b)(2), but
14 only with respect to the information contained in the
15 disclosure.

16 “(b) VIDEO, BOOK, OR RECORDED MUSIC RENTAL,
17 SALE, OR DELIVERY.—

18 “(1) IN GENERAL.—A video provider, book
19 dealer, or recorded music dealer who knowingly dis-
20 closes, to any person, personally identifiable informa-
21 tion concerning any consumer of such provider or
22 seller, as the case may be, shall be liable to the ag-
23 grieved person for the relief provided in subsection
24 (d).

1 “(2) DISCLOSURE.—A video provider, book
2 dealer, or recorded music dealer may disclose per-
3 sonally identifiable information concerning any
4 consumer—

5 “(A) to the consumer;

6 “(B) to any person with the informed,
7 written consent of the consumer given at the
8 time the disclosure is sought;

9 “(C) to a law enforcement agency pursuant
10 to a warrant issued under the Federal Rules of
11 Criminal Procedure, an equivalent State war-
12 rant, or a court order issued in accordance with
13 paragraph (4);

14 “(D) to any person if the disclosure is sole-
15 ly of the names and addresses of consumers
16 and if—

17 “(i) the video provider, book dealer, or
18 recorded music dealer, as the case may be,
19 has provided the consumer, in a clear and
20 conspicuous manner, with the opportunity
21 to prohibit such disclosure; and

22 “(ii) the disclosure does not identify
23 the title, description, or subject matter of
24 any video or other audio-visual material,

1 books, magazines, or other printed mate-
2 rial, or recorded music;

3 “(E) to any person if the disclosure is inci-
4 dent to the ordinary course of business of the
5 video provider, book dealer, or recorded music
6 dealer; or

7 “(F) pursuant to a court order, in a civil
8 proceeding upon a showing of compelling need
9 for the information that cannot be accommo-
10 dated by any other means, if—

11 “(i) the consumer is given reasonable
12 notice, by the person seeking the disclo-
13 sure, of the court proceeding relevant to
14 the issuance of the court order; and

15 “(ii) the consumer is afforded the op-
16 portunity to appear and contest the claim
17 of the person seeking the disclosure.

18 “(3) SAFEGUARDS.—If an order is granted pur-
19 suant to subparagraph (C) or (F) of paragraph (2),
20 the court shall impose appropriate safeguards
21 against unauthorized disclosure.

22 “(4) COURT ORDERS.—A court order author-
23 izing disclosure under paragraph (2)(C) shall issue
24 only with prior notice to the consumer and only if
25 the law enforcement agency shows that there is

1 probable cause to believe that a person has engaged,
2 is engaging, or is about to engage in criminal activ-
3 ity and that the records or other information sought
4 are material to the investigation of such activity. In
5 the case of a State government authority, such a
6 court order shall not issue if prohibited by the law
7 of such State. A court issuing an order pursuant to
8 this subsection, on a motion made promptly by the
9 video provider, book dealer, or recorded music deal-
10 er, may quash or modify such order if the informa-
11 tion or records requested are unreasonably volumi-
12 nous in nature or if compliance with such order oth-
13 erwise would cause an unreasonable burden on such
14 video provider, book dealer, or recorded music deal-
15 er, as the case may be.”.

16 (b) CONFORMING AMENDMENTS.—

17 (1) Subsections (c) through (f) of section 2701
18 of title 18, United States Code, are amended by
19 striking “video tape service provider” each place it
20 appears and inserting “video provider”.

21 (2) The item relating to section 2701 in the
22 analysis for chapter 121 of title 18, United States
23 Code, is amended to read as follows:

“2710. Wrongful disclosure of information about video, book, or recorded music
rental or sales.”.

1 **SEC. 202. EFFECTIVE DATE.**

2 The amendments made by section 201 take effect 12
3 months after the date of enactment of this Act.

4 **TITLE III—ENFORCEMENT AND**
5 **REMEDIES**

6 **SEC. 301. ENFORCEMENT.**

7 Except as provided in section 302(b) and section
8 2710(d) of title 18, United States Code, this Act shall be
9 enforced by the Federal Trade Commission. Except as
10 otherwise provided in this Act, a violation of this Act may
11 be punished in the same manner as a violation of a regula-
12 tion of the Federal Trade Commission.

13 **SEC. 302. VIOLATION IS UNFAIR OR DECEPTIVE ACT OR**
14 **PRACTICE.**

15 (a) IN GENERAL.—The violation of any provision of
16 title I is an unfair or deceptive act or practice proscribed
17 by section 18(a)(1)(B) of the Federal Trade Commission
18 Act (15 U.S.C. 57a(a)(1)(B)).

19 (b) ENFORCEMENT BY CERTAIN OTHER AGEN-
20 CIES.—Compliance with title I of this Act shall be en-
21 forced under—

22 (1) section 8 of the Federal Deposit Insurance
23 Act (12 U.S.C. 1818), in the case of—

24 (A) national banks, and Federal branches
25 and Federal agencies of foreign banks, by the
26 Office of the Comptroller of the Currency;

1 (B) member banks of the Federal Reserve
2 System (other than national banks), branches
3 and agencies of foreign banks (other than Fed-
4 eral branches, Federal agencies, and insured
5 State branches of foreign banks), commercial
6 lending companies owned or controlled by for-
7 eign banks, and organizations operating under
8 section 25 or 25(a) of the Federal Reserve Act
9 (12 U.S.C. 601 et seq. and 611 et seq.), by the
10 Board; and

11 (C) banks insured by the Federal Deposit
12 Insurance Corporation (other than members of
13 the Federal Reserve System) and insured State
14 branches of foreign banks, by the Board of Di-
15 rectors of the Federal Deposit Insurance Cor-
16 poration;

17 (2) section 8 of the Federal Deposit Insurance
18 Act (12 U.S.C. 1818), by the Director of the Office
19 of Thrift Supervision, in the case of a savings asso-
20 ciation the deposits of which are insured by the Fed-
21 eral Deposit Insurance Corporation;

22 (3) the Federal Credit Union Act (12 U.S.C.
23 1751 et seq.) by the National Credit Union Adminis-
24 tration Board with respect to any Federal credit
25 union;

1 (4) part A of subtitle VII of title 49, United
2 States Code, by the Secretary of Transportation
3 with respect to any air carrier or foreign air carrier
4 subject to that part;

5 (5) the Packers and Stockyards Act, 1921 (7
6 U.S.C. 181 et seq.) (except as provided in section
7 406 of that Act (7 U.S.C. 226, 227)), by the Sec-
8 retary of Agriculture with respect to any activities
9 subject to that Act; and

10 (6) the Farm Credit Act of 1971 (12 U.S.C.
11 2001 et seq.) by the Farm Credit Administration
12 with respect to any Federal land bank, Federal land
13 bank association, Federal intermediate credit bank,
14 or production credit association.

15 (c) EXERCISE OF CERTAIN POWERS.—For the pur-
16 pose of the exercise by any agency referred to in sub-
17 section (b) of its powers under any Act referred to in that
18 subsection, a violation of title I is deemed to be a violation
19 of a requirement imposed under that Act. In addition to
20 its powers under any provision of law specifically referred
21 to in subsection (b), each of the agencies referred to in
22 that subsection may exercise, for the purpose of enforcing
23 compliance with any requirement imposed under title I of
24 this Act, any other authority conferred on it by law.

1 (d) ACTIONS BY THE COMMISSION.—The Commis-
2 sion shall prevent any person from violating title I in the
3 same manner, by the same means, and with the same ju-
4 risdiction, powers, and duties as though all applicable
5 terms and provisions of the Federal Trade Commission
6 Act (15 U.S.C. 41 et seq.) were incorporated into and
7 made a part of this Act. Any entity that violates any provi-
8 sion of that title is subject to the penalties and entitled
9 to the privileges and immunities provided in the Federal
10 Trade Commission Act in the same manner, by the same
11 means, and with the same jurisdiction, power, and duties
12 as though all applicable terms and provisions of the Fed-
13 eral Trade Commission Act were incorporated into and
14 made a part of that title.

15 (e) EFFECT ON OTHER LAWS.—

16 (1) PRESERVATION OF COMMISSION AUTHOR-
17 ITY.—Nothing contained in this title shall be con-
18 strued to limit the authority of the Commission
19 under any other provision of law.

20 (2) RELATION TO COMMUNICATIONS ACT.—
21 Nothing in title I requires an operator of a website
22 or online service to take any action that is incon-
23 sistent with the requirements of section 222 or 631
24 of the Communications Act of 1934 (47 U.S.C. 222
25 or 551, respectively).

1 **SEC. 303. PRIVATE RIGHT OF ACTION.**

2 (a) PRIVATE RIGHT OF ACTION.—A person whose
3 personally identifiable information is collected, disclosed or
4 used, or is likely to be disclosed or used, in violation of
5 title I may, if otherwise permitted by the laws or rules
6 of court of a State, bring in an appropriate court of that
7 State—

8 (1) an action to enjoin or restrain such viola-
9 tion;

10 (2) an action to recover for actual monetary
11 loss from such a violation, or to receive \$5,000 in
12 damages for each such violation, whichever is great-
13 er; or

14 (3) both such actions.

15 (b) WILLFUL AND KNOWING VIOLATIONS.—If the
16 court finds that the defendant willfully or knowingly vio-
17 lated title I, the court may, in its discretion, increase the
18 amount of the award available under subsection (a)(2) to
19 \$50,000.

20 (c) EXCEPTION.—Neither an action to enjoin or re-
21 strain a violation, nor an action to recover for loss or dam-
22 age, may be brought under this section for the accidental
23 disclosure of information if the disclosure was caused by
24 an Act of God, network or systems failure, or other event
25 beyond the control of the Internet service provider, online
26 service provider, or operator of a commercial website if

1 the provider or operator took reasonable precautions to
 2 prevent such disclosure in the event of such a failure or
 3 other event.

4 (d) ATTORNEYS FEES; PUNITIVE DAMAGES.—Not-
 5 withstanding subsection (a)(2), the court in an action
 6 brought under this section, may award reasonable attor-
 7 neys fees and punitive damages to the prevailing party.

8 **SEC. 304. ACTIONS BY STATES.**

9 (a) IN GENERAL.—

10 (1) CIVIL ACTIONS.—In any case in which the
 11 attorney general of a State has reason to believe
 12 that an interest of the residents of that State has
 13 been or is threatened or adversely affected by the
 14 engagement of any person in a practice that violates
 15 title I, the State, as *parens patriae*, may bring a civil
 16 action on behalf of the residents of the State in a
 17 district court of the United States of appropriate ju-
 18 risdiction to—

19 (A) enjoin that practice;

20 (B) enforce compliance with the rule;

21 (C) obtain damage, restitution, or other
 22 compensation on behalf of residents of the
 23 State; or

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

1 (2) NOTICE.—

2 (A) IN GENERAL.—Before filing an action
3 under paragraph (1), the attorney general of
4 the State involved shall provide to the
5 Commission—

6 (i) written notice of that action; and

7 (ii) a copy of the complaint for that
8 action.

9 (B) EXEMPTION.—

10 (i) IN GENERAL.—Subparagraph (A)
11 shall not apply with respect to the filing of
12 an action by an attorney general of a State
13 under this subsection, if the attorney gen-
14 eral determines that it is not feasible to
15 provide the notice described in that sub-
16 paragraph before the filing of the action.

17 (ii) NOTIFICATION.—In an action de-
18 scribed in clause (i), the attorney general
19 of a State shall provide notice and a copy
20 of the complaint to the Commission at the
21 same time as the attorney general files the
22 action.

23 (b) INTERVENTION.—

24 (1) IN GENERAL.—On receiving notice under
25 subsection (a)(2), the Commission shall have the

1 right to intervene in the action that is the subject
2 of the notice.

3 (2) EFFECT OF INTERVENTION.—If the Com-
4 mission intervenes in an action under subsection (a),
5 it shall have the right—

6 (A) to be heard with respect to any matter
7 that arises in that action; and

8 (B) to file a petition for appeal.

9 (c) CONSTRUCTION.—For purposes of bringing any
10 civil action under subsection (a), nothing in this Act shall
11 be construed to prevent an attorney general of a State
12 from exercising the powers conferred on the attorney gen-
13 eral by the laws of that State to—

14 (1) conduct investigations;

15 (2) administer oaths or affirmations; or

16 (3) compel the attendance of witnesses or the
17 production of documentary and other evidence.

18 (d) ACTIONS BY THE COMMISSION.—In any case in
19 which an action is instituted by or on behalf of the Com-
20 mission for violation of title I, no State may, during the
21 pendency of that action, institute an action under sub-
22 section (a) against any defendant named in the complaint
23 in that action for violation of that rule.

24 (e) VENUE; SERVICE OF PROCESS.—

1 (1) VENUE.—Any action brought under sub-
2 section (a) may be brought in the district court of
3 the United States that meets applicable require-
4 ments relating to venue under section 1391 of title
5 28, United States Code.

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

9 (A) is an inhabitant; or

10 (B) may be found.

11 **SEC. 305. WHISTLEBLOWER PROTECTION.**

12 (a) IN GENERAL.—No Internet service provider, on-
13 line service provider, or commercial website operator may
14 discharge or otherwise discriminate against any employee
15 with respect to compensation, terms, conditions, or privi-
16 leges of employment because the employee (or any person
17 acting pursuant to the request of the employee) provided
18 information to any Federal or State agency or to the At-
19 torney General of the United States or of any State re-
20 garding a possible violation of any provision of title I.

21 (b) ENFORCEMENT.—Any employee or former em-
22 ployee who believes he has been discharged or discrimi-
23 nated against in violation of subsection (a) may file a civil
24 action in the appropriate United States district court be-
25 fore the close of the 2-year period beginning on the date

1 of such discharge or discrimination. The complainant shall
2 also file a copy of the complaint initiating such action with
3 the appropriate Federal agency.

4 (c) REMEDIES.—If the district court determines that
5 a violation of subsection (a) has occurred, it may order
6 the Internet service provider, online service provider, or
7 commercial website operator that committed the
8 violation—

9 (1) to reinstate the employee to his former posi-
10 tion;

11 (2) to pay compensatory damages; or

12 (3) take other appropriate actions to remedy
13 any past discrimination.

14 (d) ATTORNEYS FEES; PUNITIVE DAMAGES.—Not-
15 withstanding subsection (c)(2), the court in an action
16 brought under this section, may award reasonable attor-
17 neys fees and punitive damages to the prevailing party.

18 (e) LIMITATION.—The protections of this section
19 shall not apply to any employee who—

20 (1) deliberately causes or participates in the al-
21 leged violation; or

22 (2) knowingly or recklessly provides substan-
23 tially false information to such an agency or the At-
24 torney General.

1 (f) BURDENS OF PROOF.—The legal burdens of proof
2 that prevail under subchapter III of chapter 12 of title
3 5, United States Code (5 U.S.C. 1221 et seq.) shall govern
4 adjudication of protected activities under this section.

5 **SEC. 306. NO EFFECT ON OTHER REMEDIES.**

6 The remedies provided by this sections 303 and 304
7 are in addition to any other remedy available under any
8 provision of law.

9 **SEC. 307. FTC OFFICE OF ONLINE PRIVACY.**

10 The Federal Trade Commission shall establish an Of-
11 fice of Online Privacy headed by a senior level position
12 officer who reports directly to the Commission and its
13 General Counsel. The Office shall study privacy issues as-
14 sociated with electronic commerce and the Internet, the
15 operation of this Act and the effectiveness of the privacy
16 protections provided by title I. The Office shall report its
17 findings and recommendations from time to time to the
18 Commission, and, notwithstanding any law, regulation, or
19 executive order to the contrary, shall submit an annual
20 report directly to the Senate Committee on Commerce,
21 Science, and Transportation and the House of Represent-
22 atives Committee on Commerce on the status of online and
23 Internet privacy issues, together with any recommenda-
24 tions for additional legislation relating to those issues.

1 **TITLE IV—COMMUNICATIONS**
2 **TECHNOLOGY PRIVACY PRO-**
3 **TECTIONS**

4 **SEC. 401. PRIVACY PROTECTION FOR SUBSCRIBERS OF**
5 **SATELLITE TELEVISION SERVICES FOR PRI-**
6 **VATE HOME VIEWING.**

7 (a) IN GENERAL.—Section 631 of the Communica-
8 tions Act of 1934 (47 U.S.C. 551) is amended to read
9 as follows:

10 **“SEC. 631. PRIVACY OF SUBSCRIBER INFORMATION FOR**
11 **SUBSCRIBERS OF CABLE SERVICE AND SAT-**
12 **ELLITE TELEVISION SERVICE.**

13 “(a) NOTICE TO SUBSCRIBERS REGARDING PERSON-
14 ALLY IDENTIFIABLE INFORMATION.—At the time of en-
15 tering into an agreement to provide any cable service, sat-
16 ellite home viewing service, or other service to a sub-
17 scriber, and not less often than annually thereafter, a
18 cable operator, satellite carrier, or distributor shall provide
19 notice in the form of a separate, written statement to such
20 subscriber that clearly and conspicuously informs the sub-
21 scriber of—

22 “(1) the nature of personally identifiable infor-
23 mation collected or to be collected with respect to
24 the subscriber as a result of the provision of such

1 service and the nature of the use of such informa-
2 tion;

3 “(2) the nature, frequency, and purpose of any
4 disclosure that may be made of such information, in-
5 cluding an identification of the types of persons to
6 whom the disclosure may be made;

7 “(3) the period during which such information
8 will be maintained by the cable operator, satellite
9 carrier, or distributor;

10 “(4) the times and place at which the sub-
11 scriber may have access to such information in ac-
12 cordance with subsection (d); and

13 “(5) the limitations provided by this section
14 with respect to the collection and disclosure of infor-
15 mation by the cable operator, satellite carrier, or dis-
16 tributor and the right of the subscriber under this
17 section to enforce such limitations.

18 “(b) COLLECTION OF PERSONALLY IDENTIFIABLE
19 INFORMATION.—

20 “(1) IN GENERAL.—Except as provided in para-
21 graph (2), a cable operator, satellite carrier, or dis-
22 tributor shall not use its cable or satellite system to
23 collect personally identifiable information concerning
24 any subscriber without the prior written or electronic
25 consent of the subscriber.

1 “(2) EXCEPTION.—A cable operator, satellite
2 carrier, or distributor may use its cable or satellite
3 system to collect information described in paragraph
4 (1) in order to—

5 “(A) obtain information necessary to
6 render a cable or satellite service or other serv-
7 ice provided by the cable operator, satellite car-
8 rier, or distributor to the subscriber; or

9 “(B) detect unauthorized reception of cable
10 or satellite communications.

11 “(c) DISCLOSURE OF PERSONALLY IDENTIFIABLE
12 INFORMATION.—

13 “(1) IN GENERAL.—Except as provided in para-
14 graph (2), a cable operator, satellite carrier, or dis-
15 tributor may not disclose personally identifiable in-
16 formation concerning any subscriber without the
17 prior written or electronic consent of the subscriber
18 and shall take such actions as are necessary to pre-
19 vent unauthorized access to such information by a
20 person other than the subscriber or the cable oper-
21 ator, satellite carrier, or distributor.

22 “(2) EXCEPTIONS.—A cable operator, satellite
23 carrier, or distributor may disclose information de-
24 scribed in paragraph (1) if the disclosure is—

1 “(A) necessary to render, or conduct a le-
2 gitimate business activity related to, a cable or
3 satellite service or other service provided by the
4 cable operator, satellite carrier, or distributor to
5 the subscriber;

6 “(B) subject to paragraph (3), made pur-
7 suant to a court order authorizing such disclo-
8 sure, if the subscriber is notified of such order
9 by the person to whom the order is directed; or

10 “(C) a disclosure of the names and ad-
11 dresses of subscribers to any other provider of
12 cable or satellite service or other service, if—

13 “(i) the cable operator, satellite car-
14 rier, or distributor has provided the sub-
15 scriber the opportunity to prohibit or limit
16 such disclosure; and

17 “(ii) the disclosure does not reveal, di-
18 rectly or indirectly—

19 “(I) the extent of any viewing or
20 other use by the subscriber of a cable
21 or satellite service or other service
22 provided by the cable operator, sat-
23 ellite carrier, or distributor; or

24 “(II) the nature of any trans-
25 action made by the subscriber over

1 the cable or satellite system of the
2 cable operator, satellite carrier, or dis-
3 tributor.

4 “(3) COURT ORDERS.—A governmental entity
5 may obtain personally identifiable information con-
6 cerning a cable or satellite subscriber pursuant to a
7 court order only if, in the court proceeding relevant
8 to such court order—

9 “(A) such entity offers clear and con-
10 vincing evidence that the subject of the infor-
11 mation is reasonably suspected of engaging in
12 criminal activity and that the information
13 sought would be material evidence in the case;
14 and

15 “(B) the subject of the information is af-
16 forded the opportunity to appear and contest
17 such entity’s claim.

18 “(d) SUBSCRIBER ACCESS TO INFORMATION.—A
19 cable or satellite subscriber shall be provided access to all
20 personally identifiable information regarding that sub-
21 scriber that is collected and maintained by a cable oper-
22 ator, satellite carrier, or distributor. Such information
23 shall be made available to the subscriber at reasonable
24 times and at a convenient place designated by such cable
25 operator, satellite carrier, or distributor. A cable or sat-

1 elite subscriber shall be provided reasonable opportunity
2 to correct any error in such information.

3 “(e) DESTRUCTION OF INFORMATION.—A cable oper-
4 ator, satellite carrier, or distributor shall destroy person-
5 ally identifiable information if the information is no longer
6 necessary for the purpose for which it was collected and
7 there are no pending requests or orders for access to such
8 information under subsection (d) or pursuant to a court
9 order.

10 “(f) RELIEF.—

11 “(1) IN GENERAL.—Any person aggrieved by
12 any act of a cable operator, satellite carrier, or dis-
13 tributor in violation of this section may bring a civil
14 action in a district court of the United States.

15 “(2) DAMAGES AND COSTS.—In any action
16 brought under paragraph (1), the court may award
17 a prevailing plaintiff—

18 “(A) actual damages but not less than liq-
19 uidated damages computed at the rate of \$100
20 a day for each day of violation or \$1,000,
21 whichever is greater;

22 “(B) punitive damages; and

23 “(C) reasonable attorneys’ fees and other
24 litigation costs reasonably incurred.

1 “(3) NO EFFECT ON OTHER REMEDIES.—The
2 remedy provided by this subsection shall be in addi-
3 tion to any other remedy available under any provi-
4 sion of law to a cable or satellite subscriber.

5 “(g) DEFINITIONS.—In this section:

6 “(1) DISTRIBUTOR.—The term ‘distributor’
7 means an entity that contracts to distribute sec-
8 ondary transmissions from a satellite carrier and, ei-
9 ther as a single channel or in a package with other
10 programming, provides the secondary transmission
11 either directly to individual subscribers for private
12 home viewing or indirectly through other program
13 distribution entities.

14 “(2) CABLE OPERATOR.—

15 “(A) IN GENERAL.—The term ‘cable oper-
16 ator’ has the meaning given that term in sec-
17 tion 602.

18 “(B) INCLUSION.—The term includes any
19 person who—

20 “(i) is owned or controlled by, or
21 under common ownership or control with,
22 a cable operator; and

23 “(ii) provides any wire or radio com-
24 munications service.

1 “(3) OTHER SERVICE.—The term ‘other serv-
2 ice’ includes any wire, electronic, or radio commu-
3 nications service provided using any of the facilities
4 of a cable operator, satellite carrier, or distributor
5 that are used in the provision of cable service or sat-
6 ellite home viewing service.

7 “(4) PERSONALLY IDENTIFIABLE INFORMA-
8 TION.—The term ‘personally identifiable informa-
9 tion’ does not include any record of aggregate data
10 that does not identify particular persons.

11 “(5) SATELLITE CARRIER.—The term ‘satellite
12 carrier’ means an entity that uses the facilities of a
13 satellite or satellite service licensed by the Federal
14 Communications Commission and operates in the
15 Fixed-Satellite Service under part 25 of title 47 of
16 the Code of Federal Regulations or the Direct
17 Broadcast Satellite Service under part 100 of title
18 47 of the Code of Federal Regulations, to establish
19 and operate a channel of communications for point-
20 to-multipoint distribution of television station sig-
21 nals, and that owns or leases a capacity or service
22 on a satellite in order to provide such point-to-
23 multipoint distribution, except to the extent that
24 such entity provides such distribution pursuant to

1 tariff under the Communications Act of 1934, other
2 than for private home viewing.”.

3 (b) NOTICE WITH RESPECT TO CERTAIN AGREE-
4 MENTS.—

5 (1) IN GENERAL.—Except as provided in para-
6 graph (2), a cable operator, satellite carrier, or dis-
7 tributor who has entered into agreements referred to
8 in section 631(a) of the Communications Act of
9 1934, as amended by subsection (a), before the date
10 of enactment of this Act, shall provide any notice re-
11 quired under that section, as so amended, to sub-
12 scribers under such agreements not later than 180
13 days after that date.

14 (2) EXCEPTION.—Paragraph (1) shall not
15 apply with respect to any agreement under which a
16 cable operator, satellite carrier, or distributor was
17 providing notice under section 631(a) of the Com-
18 munications Act of 1934, as in effect on the day be-
19 fore the date of enactment of this Act, as of such
20 date.

21 **SEC. 402. CUSTOMER PROPRIETARY NETWORK INFORMA-**
22 **TION.**

23 Section 222 (c)(1) of the Communications Act of
24 1934 (47 U.S.C. 222 (c)(1)) is amended by striking “ap-
25 proval” and inserting “express prior authorization”.

1 (B) in the case of consumers who are chil-
2 dren, the abilities described in clauses (i), (ii),
3 and (iii) of subparagraph (A) are or can be ex-
4 ercised by their parents; and

5 (C) changes in the Commission's regula-
6 tions could provide greater assurance of the off-
7 line privacy rights and remedies of parents and
8 consumers generally;

9 (2) review responses and suggestions from af-
10 fected commercial and nonprofit entities to changes
11 proposed under paragraph (1)(C); and

12 (3) make recommendations to the Congress for
13 any legislative changes necessary to ensure such
14 rights and remedies.

15 (b) SCHEDULE FOR FEDERAL TRADE COMMISSION
16 RESPONSES.—The Federal Trade Commission shall, with-
17 in 6 months after the date of enactment of this Act, sub-
18 mit to Congress a report containing the recommendations
19 required by subsection (a)(3).

20 **SEC. 502. FEDERAL COMMUNICATIONS COMMISSION RULE-**
21 **MAKING.**

22 (a) PROCEEDING REQUIRED.—The Federal Commu-
23 nications Commission shall initiate a rulemaking pro-
24 ceeding to establish uniform consumer privacy rules for

1 all communications providers. The rulemaking proceeding
2 shall—

3 (1) examine the privacy rights and remedies of
4 the consumers of all online and offline technologies,
5 including telecommunications providers, cable,
6 broadcast, satellite, wireless, and telephony services;

7 (2) determine whether consumers are able, and,
8 if not, the methods by which consumers may be en-
9 abled to exercise such rights and remedies; and

10 (3) change the Commission's regulations to co-
11 ordinate, rationalize, and harmonize laws and regu-
12 lations administered by the Commission that relate
13 to those rights and remedies.

14 (b) DEADLINE FOR CHANGES.—The Federal Com-
15 munications Commission shall complete the rulemaking
16 within 6 months after the date of enactment of this Act.

17 **SEC. 503. DEPARTMENT OF LABOR STUDY OF EMPLOYEE-**
18 **MONITORING ACTIVITIES.**

19 The Secretary of Labor shall study the extent and
20 nature of employer practices that involving monitoring em-
21 ployee activities both at the workplace and away from the
22 workplace, by electronic or other remote means, including
23 surveillance of electronic mail and Internet use, to deter-
24 mine whether and to what extent such practices constitute
25 an inappropriate violation of employee privacy. The Sec-

1 retary shall report the results of the study, including find-
 2 ings and recommendations, if any, for legislation or regu-
 3 lation to the Congress within 6 months after the date of
 4 enactment of this Act.

5 **TITLE VI—PROTECTION OF PER-**
 6 **SONALLY IDENTIFIABLE IN-**
 7 **FORMATION IN BANKRUPTCY**

8 **SEC. 601. PERSONALLY IDENTIFIABLE INFORMATION NOT**
 9 **ASSET IN BANKRUPTCY.**

10 Section 541(b) of title 11, United States Code, is
 11 amended—

12 (1) by striking “or” after the semicolon in
 13 paragraph (4)(B)(ii);

14 (2) by striking “prohibition.” in paragraph (5)
 15 and inserting “prohibition; or”; and

16 (3) by inserting after paragraph (5) the fol-
 17 lowing:

18 “(6) any personally identifiable information (as
 19 defined in section 901(6) of the Consumer Privacy
 20 Protection Act), or any compilation, or record (in
 21 electronic or any other form) of such information.”.

22 **TITLE VII—INTERNET SECURITY**
 23 **INITIATIVES**

24 **SEC. 701. FINDINGS.**

25 The Congress finds the following:

1 (1) Good computer security practices are an un-
2 derpinning of any privacy protection. The operator
3 of a computer system should protect that system
4 from unauthorized use and secure any private, per-
5 sonal information.

6 (2) The Federal Government should be a role
7 model in securing its computer systems and should
8 ensure the protection of private, personal informa-
9 tion controlled by Federal agencies.

10 (3) The National Institute of Standards and
11 Technology has the responsibility for developing
12 standards and guidelines needed to ensure the cost-
13 effective security and privacy of private, personal in-
14 formation in Federal computer systems.

15 (4) This Nation faces a shortage of trained,
16 qualified information technology workers, including
17 computer security professionals. As the demand for
18 information technology workers grows, the Federal
19 government will have an increasingly difficult time
20 attracting such workers into the Federal workforce.

21 (5) Some commercial off-the-shelf hardware and
22 off-the-shelf software components to protect com-
23 puter systems are widely available. There is still a
24 need for long-term computer security research, par-
25 ticularly in the area of infrastructure protection.

1 (6) The Nation's information infrastructures
2 are owned, for the most part, by the private sector,
3 and partnerships and cooperation will be needed for
4 the security of these infrastructures.

5 (7) There is little financial incentive for private
6 companies to enhance the security of the Internet
7 and other infrastructures as a whole. The Federal
8 government will need to make investments in this
9 area to address issues and concerns not addressed
10 by the private sector.

11 **SEC. 702. COMPUTER SECURITY PARTNERSHIP COUNCIL.**

12 (a) ESTABLISHMENT.—The Secretary of Commerce,
13 in consultation with the President's Information Tech-
14 nology Advisory Committee established by Executive
15 Order No. 13035 of February 11, 1997 (62 F.R. 7231),
16 shall establish a 25-member Computer Security Partner-
17 ship Council.

18 (b) CHAIRMAN; MEMBERSHIP.—The Council shall
19 have a chairman, appointed by the Secretary, and 24 addi-
20 tional members, appointed by the Secretary as follows:

21 (1) 5 members, who are not officers or employ-
22 ees of the United States, who are recognized as lead-
23 ers in the networking and computer security busi-
24 ness, at least 1 of whom represents a small or me-
25 dium-sized company.

1 (2) 5 members, who are—

2 (A) not officers or employees of the United
3 States, and

4 (B) not in the networking and computer
5 security business,

6 at least 1 of whom represents a small or medium-
7 sized company.

8 (3) 5 members, who are not officers or employ-
9 ees of the United States, who represent public inter-
10 est groups or State or local governments, of whom
11 at least 2 represent such groups and at least 2 rep-
12 resent such governments.

13 (4) 5 members, who are not officers or employ-
14 ees of the United States, affiliated with a college,
15 university, or other academic, research-oriented, or
16 public policy institution, with recognized expertise in
17 the field of networking and computer security, whose
18 primary source of employment is by that college,
19 university, or other institution rather than a busi-
20 ness organization involved in the networking and
21 computer security business.

22 (5) 4 members, who are officers or employees of
23 the United States, with recognized expertise in com-
24 puter systems management, including computer and
25 network security.

1 (c) FUNCTION.—The Council shall collect and share
2 information about, and increase public awareness of, infor-
3 mation security practices and programs, threats to infor-
4 mation security, and responses to those threats.

5 (d) STUDY.—Within 12 months after the date of en-
6 actment of this Act, the Council shall publish a report
7 which evaluates and describes areas of computer security
8 research and development that are not adequately devel-
9 oped or funded.

10 (e) ADDITIONAL RECOMMENDATIONS.—The Council
11 shall periodically make recommendations to appropriate
12 government and private sector entities for enhancing the
13 security of networked computers operated or maintained
14 by those entities.

15 **SEC. 703. RESEARCH AND DEVELOPMENT.**

16 Section 20 of the National Institute of Standards and
17 Technology Act (15 U.S.C. 278g–3) is amended—

18 (1) by redesignating subsections (c) and (d) as
19 subsections (d) and (e), respectively; and

20 (2) by inserting after subsection (b) the fol-
21 lowing:

22 “(c) RESEARCH AND DEVELOPMENT OF PROTECTION
23 TECHNOLOGIES.—

24 “(1) IN GENERAL.—The Institute shall estab-
25 lish a program at the National Institute of Stand-

1 ards and Technology to conduct, or to fund the con-
2 duct of, research and development of technology and
3 techniques to provide security for advanced commu-
4 nications and computing systems and networks in-
5 cluding the Next Generation Internet, the underlying
6 structure of the Internet, and networked computers.

7 “(2) PURPOSE.—A purpose of the program es-
8 tablished under paragraph (1) is to address issues or
9 problems that are not addressed by market-driven,
10 private-sector information security research. This
11 may include research—

12 “(A) to identify Internet security problems
13 which are not adequately addressed by current
14 security technologies;

15 “(B) to develop interactive tools to analyze
16 security risks in an easy-to-understand manner;

17 “(C) to enhance the security and reliability
18 of the underlying Internet infrastructure while
19 minimizing any adverse operational impacts
20 such as speed; and

21 “(D) to allow networks to become self-heal-
22 ing and provide for better analysis of the state
23 of Internet and infrastructure operations and
24 security.

1 “(3) MATCHING GRANTS.—A grant awarded by
 2 the Institute under the program established under
 3 paragraph (1) to a commercial enterprise may not
 4 exceed 50 percent of the cost of the project to be
 5 funded by the grant.

6 “(4) AUTHORIZATION OF APPROPRIATIONS.—
 7 There are authorized to be appropriated to the Insti-
 8 tute to carry out this subsection—

9 “(A) \$50,000,000 for fiscal year 2001;

10 “(B) \$60,000,000 for fiscal year 2002;

11 “(C) \$70,000,000 for fiscal year 2003;

12 “(D) \$80,000,000 for fiscal year 2004;

13 “(E) \$90,000,000 for fiscal year 2005; and

14 “(F) \$100,000,000 for fiscal year 2006.”.

15 **SEC. 704. COMPUTER SECURITY TRAINING PROGRAMS.**

16 (a) IN GENERAL.—The Secretary of Commerce, in
 17 consultation with appropriate Federal agencies, shall es-
 18 tablish a program to support the training of individuals
 19 in computer security, Internet security, and related fields
 20 at institutions of higher education located in the United
 21 States.

22 (b) SUPPORT AUTHORIZED.—Under the program es-
 23 tablished under subsection (a), the Secretary may provide
 24 scholarships, loans, and other forms of financial aid to stu-
 25 dents at institutions of higher education. The Secretary

1 shall require a recipient of a scholarship under this pro-
2 gram to provide a reasonable period of service as an em-
3 ployee of the United States government after graduation
4 as a condition of the scholarship, and may authorize full
5 or partial forgiveness of indebtedness for loans made
6 under this program in exchange for periods of employment
7 by the United States government.

8 (c) AUTHORIZATION OF APPROPRIATIONS.—There
9 are authorized to be appropriated to the Secretary such
10 sums as may be necessary to carry out this section—

11 (A) \$15,000,000 for fiscal year 2001;

12 (B) \$17,000,000 for fiscal year 2002;

13 (C) \$20,000,000 for fiscal year 2003;

14 (D) \$25,000,000 for fiscal year 2004;

15 (E) \$30,000,000 for fiscal year 2005; and

16 (F) \$35,000,000 for fiscal year 2006.

17 **SEC. 705. GOVERNMENT INFORMATION SECURITY STAND-**
18 **ARDS.**

19 (a) IN GENERAL.—Section 20(b) of the National In-
20 stitute of Standards and Technology Act (15 U.S.C. 278g-
21 3(b)) is amended—

22 (1) by striking “and” after the semicolon in
23 paragraph (4);

24 (2) by redesignating paragraph (5) as para-
25 graph (6); and

1 (3) by inserting after paragraph (4) the fol-
2 lowing:

3 “(5) to provide guidance and assistance to Fed-
4 eral agencies in the protection of interconnected
5 computer systems and to coordinate Federal re-
6 sponse efforts related to unauthorized access to Fed-
7 eral computer systems; and”.

8 (b) FEDERAL COMPUTER SYSTEM SECURITY TRAIN-
9 ING.—Section 5(b) of the Computer Security Act of 1987
10 (49 U.S.C. 759 note) is amended—

11 (1) by striking “and” at the end of paragraph
12 (1);

13 (2) by striking the period at the end of para-
14 graph (2) and inserting in lieu thereof “; and”; and

15 (3) by adding at the end the following new
16 paragraph:

17 “(3) to include emphasis on protecting the
18 availability of Federal electronic citizen services and
19 protecting sensitive information in Federal databases
20 and Federal computer sites that are accessible
21 through public networks.”.

1 **SEC. 706. RECOGNITION OF QUALITY IN COMPUTER SECUR-**
2 **RITY PRACTICES.**

3 Section 20 of the National Institute of Standards and
4 Technology Act (15 U.S.C. 278g-3), as amended by sec-
5 tion 703, is further amended—

6 (1) by redesignating subsections (d) and (e) as
7 subsections (e) and (f), respectively; and

8 (2) by inserting after subsection (c), the fol-
9 lowing:

10 “(d) AWARD PROGRAM.—The Institute may establish
11 a program for the recognition of excellence in Federal
12 computer system security practices, including the develop-
13 ment of a seal, symbol, mark, or logo that could be dis-
14 played on the website maintained by the operator of such
15 a system recognized under the program. In order to be
16 recognized under the program, the operator—

17 “(1) shall have implemented exemplary proc-
18 esses for the protection of its systems and the infor-
19 mation stored on that system;

20 “(2) shall have met any standard established
21 under subsection (a);

22 “(3) shall have a process in place for updating
23 the system security procedures; and

24 “(4) shall meet such other criteria as the Insti-
25 tute may require.”.

1 **SEC. 707. DEVELOPMENT OF AUTOMATED PRIVACY CON-**
 2 **TROLS.**

3 Section 20 of the National Institute of Standards and
 4 Technology Act (15 U.S.C. 278g-3), as amended by sec-
 5 tion 706, is further amended—

6 (1) by redesignating subsection (f) as sub-
 7 section (g); and

8 (2) by inserting after subsection (e) the fol-
 9 lowing:

10 “(f) DEVELOPMENT OF INTERNET PRIVACY PRO-
 11 GRAM.—The Institute shall encourage and support the de-
 12 velopment of one or more computer programs, protocols,
 13 or other software, such as the World Wide Web Consor-
 14 tium’s P3P program, capable of being installed on com-
 15 puters, or computer networks, with Internet access that
 16 would reflect the user’s preferences for protecting person-
 17 ally-identifiable or other sensitive, privacy-related informa-
 18 tion, and automatically execute the program, once acti-
 19 vated, without requiring user intervention.”.

20 **TITLE VIII—CONGRESSIONAL IN-**
 21 **FORMATION SECURITY**
 22 **STANDARDS**

23 **SEC. 801. EXERCISE OF RULEMAKING POWER.**

24 This title is enacted by the Congress—

25 (1) as an exercise of the rulemaking power of
 26 the House of Representatives and the Senate, re-

1 spectively, and as such it is deemed a part of the
2 rules of each House, respectively, but applicable only
3 with respect to that House; and it supersedes other
4 rules only to the extent that it are inconsistent
5 therewith; and

6 (2) with full recognition of the constitutional
7 right of either House to change the rules (so far as
8 relating to that House) at any time, in the same
9 manner and to the same extent as in the case of any
10 other rule of that House.

11 **SEC. 802. SENATE.**

12 (a) IN GENERAL.—The Sergeant at Arms of the
13 United States Senate shall develop regulations setting
14 forth an information security and electronic privacy policy
15 governing use of the Internet by officers and employees
16 of the Senate in accordance with the following 4 principles
17 of privacy:

18 (1) NOTICE AND AWARENESS.—Websites must
19 provide users notice of their information practices.

20 (2) CHOICES AND CONSENT.—Websites must
21 offer users choices as to how personally identifiable
22 information is used beyond the use for which the in-
23 formation was provided.

24 (3) ACCESS AND PARTICIPATION.—Websites
25 must offer users reasonable access to personally

1 identifiable information and an opportunity to cor-
2 rect inaccuracies.

3 (4) SECURITY AND INTEGRITY.—Websites must
4 take reasonable steps to protect the security and in-
5 tegrity of personally identifiable information.

6 (b) PROCEDURE.—

7 (1) PROPOSAL.—The Sergeant at Arms shall
8 publish a general notice of proposed rulemaking
9 under section 553(b) of title 5, United States Code,
10 but, instead of publication of a general notice of pro-
11 posed rulemaking in the Federal Register, the Ser-
12 geant at Arms shall transmit such notice to the
13 President pro tempore of the Senate for publication
14 in the Congressional Record on the first day on
15 which the Senate is in session following such trans-
16 mittal. Such notice shall set forth the recommenda-
17 tions of the Sergeant at Arms for regulations under
18 subsection (a).

19 (2) COMMENT.—Before adopting regulations,
20 the Sergeant at Arms shall provide a comment pe-
21 riod of at least 30 days after publication of general
22 notice of proposed rulemaking.

23 (3) ADOPTION.—After considering comments,
24 the Sergeant at Arms shall adopt regulations and
25 shall transmit notice of such action together with a

1 copy of such regulations to the President pro tem-
2 pore of the Senate for publication in the Congres-
3 sional Record on the first day on which the Senate
4 is in session following such transmittal.

5 (c) APPROVAL OF REGULATIONS.—

6 (1) IN GENERAL.—The regulations adopted by
7 the Sergeant at Arms may be approved by the Sen-
8 ate by resolution.

9 (2) REFERRAL.—Upon receipt of a notice of
10 adoption of regulations under subsection (b)(3), the
11 presiding officers of the Senate shall refer such no-
12 tice, together with a copy of such regulations, to the
13 Committee on Rules and Administration of the Sen-
14 ate. The purpose of the referral shall be to consider
15 whether such regulations should be approved.

16 (3) JOINT REFERRAL AND DISCHARGE.—The
17 presiding officer of the Senate may refer the notice
18 of issuance of regulations, or any resolution of ap-
19 proval of regulations, to one committee or jointly to
20 more than one committee. If a committee of the
21 Senate acts to report a jointly referred measure, any
22 other committee of the Senate must act within 30
23 calendar days of continuous session, or be automati-
24 cally discharged.

1 (4) RESOLUTION OF APPROVAL.—In the case of
2 a resolution of the Senate, the matter after the re-
3 solving clause shall be the following: “the following
4 regulations issued by the Sergeant at Arms on
5 _____, 2_____ are hereby approved:”
6 (the blank spaces being appropriately filled in and
7 the text of the regulations being set forth).

8 (d) ISSUANCE AND EFFECTIVE DATE.—

9 (1) PUBLICATION.—After approval of the regu-
10 lations under subsection (c), the Sergeant at Arms
11 shall submit the regulations to the President pro
12 tempore of the Senate for publication in the Con-
13 gressional Record on the first day on which the Sen-
14 ate is in session following such transmittal.

15 (2) DATE OF ISSUANCE.—The date of issuance
16 of the regulations shall be the date on which they
17 are published in the Congressional Record under
18 paragraph (1).

19 (3) EFFECTIVE DATE.—The regulations shall
20 become effective not less than 60 days after the reg-
21 ulations are issued, except that the Sergeant at
22 Arms may provide for an earlier effective date for
23 good cause found (within the meaning of section
24 553(d)(3) of title 5, United States Code) and pub-
25 lished with the regulation.

1 (e) AMENDMENT OF REGULATIONS.—Regulations
2 may be amended in the same manner as is described in
3 this section for the adoption, approval, and issuance of
4 regulations, except that the Sergeant at Arms may dis-
5 pense with publication of a general notice of proposed rule-
6 making of minor, technical, or urgent amendments that
7 satisfy the criteria for dispensing with publication of such
8 notice pursuant to section 553(b)(B) of title 5, United
9 States Code.

10 (f) RIGHT TO PETITION FOR RULEMAKING.—Any in-
11 terested party may petition to the Sergeant at Arms for
12 the issuance, amendment, or repeal of a regulation.

13 **TITLE IX—DEFINITIONS**

14 **SEC. 901. DEFINITIONS.**

15 In this Act:

16 (1) OPERATOR OF A COMMERCIAL WEBSITE.—

17 The term “operator of a commercial website”—

18 (A) means any person who operates a
19 website located on the Internet or an online
20 service and who collects or maintains personal
21 information from or about the users of or visi-
22 tors to such website or online service, or on
23 whose behalf such information is collected or
24 maintained, where such website or online serv-
25 ice is operated for commercial purposes, includ-

1 ing any person offering products or services for
2 sale through that website or online service, in-
3 volving commerce—

4 (i) among the several States or with 1
5 or more foreign nations;

6 (ii) in any territory of the United
7 States or in the District of Columbia, or
8 between any such territory and—

9 (I) another such territory; or

10 (II) any State or foreign nation;

11 or

12 (iii) between the District of Columbia
13 and any State, territory, or foreign nation;

14 but

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

19 (2) DISCLOSE.—The term “disclose” means the
20 release of personally identifiable information about a
21 user of an Internet service, online service, or com-
22 mercial website by an Internet service provider, on-
23 line service provider, or operator of a commercial
24 website for any purpose, except where such informa-
25 tion is provided to a person who provides support for

1 the internal operations of the service or website and
2 who does not disclose or use that information for
3 any other purpose.

4 (3) RELEASE.—The term “release of personally
5 identifiable information” means the direct or indi-
6 rect, active or passive, sharing, selling, renting, or
7 other provision of personally identifiable information
8 of a user of an Internet service, online service, or
9 commercial website to any other person other than
10 the user.

11 (4) INTERNAL OPERATIONS SUPPORT.—The
12 term “support for the internal operations of a serv-
13 ice or website” means any activity necessary to
14 maintain the technical functionality of that service
15 or website.

16 (5) COLLECT.—The term “collect” means the
17 gathering of personally identifiable information
18 about a user of an Internal service, online service, or
19 commercial website by or on behalf of the provider
20 or operator of that service or website by any means,
21 direct or indirect, active or passive, including—

22 (A) an online request for such information
23 by the provider or operator, regardless of how
24 the information is transmitted to the provider
25 or operator;

1 (B) the use of a chat room, message board,
2 or other online service to gather the informa-
3 tion; or

4 (C) tracking or use of any identifying code
5 linked to a user of such a service or website, in-
6 cluding the use of cookies.

7 (3) COOKIE.—The term “cookie” means any
8 program, function, or device, commonly known as a
9 “cookie”, that makes a record on the user’s com-
10 puter (or other electronic device) of that user’s ac-
11 cess to an Internet service, online service, or com-
12 mercial website.

13 (4) FEDERAL AGENCY.—The term “Federal
14 agency” means an agency, as that term is defined
15 in section 551(1) of title 5, United States Code.

16 (5) INTERNET.—The term “Internet” means
17 collectively the myriad of computer and tele-
18 communications facilities, including equipment and
19 operating software, which comprise the inter-
20 connected world-wide network of networks that em-
21 ploy the Transmission Control Protocol/Internet
22 Protocol, or any predecessor or successor protocols
23 to such protocol, to communicate information of all
24 kinds by wire or radio.

1 (6) PERSONALLY IDENTIFIABLE INFORMA-
2 TION.—The term “personally identifiable informa-
3 tion” means individually identifiable information
4 about an individual collected online, including—

5 (A) a first and last name, whether given at
6 birth or adoption, assumed, or legally changed;

7 (B) a home or other physical address in-
8 cluding street name and name of a city or town;

9 (C) an e-mail address;

10 (D) a telephone number;

11 (E) a Social Security number;

12 (F) a credit card number;

13 (G) a birth date, birth certificate number,
14 or place of birth;

15 (H) any other identifier that the Commis-
16 sion determines permits the physical or online
17 contacting of a specific individual; or

18 (I) unique identifying information that an
19 Internet service provider, online service pro-
20 vider, or operator of a commercial website col-
21 lects and combines with an identifier described
22 in this paragraph.

23 (7) INTERNET SERVICE PROVIDER; ONLINE
24 SERVICE PROVIDER; WEBSITE.—The Commission
25 shall by rule define the terms “Internet service pro-

1 vider”, “online service provider”, and “website”, and
2 shall revise or amend such rule to take into account
3 changes in technology, practice, or procedure with
4 respect to the collection of personal information over
5 the Internet.

6 (8) OFFLINE.—The term “offline” refers to any
7 activity regulated by this Act or by section 2710 of
8 title 18, United States Code, that occurs other than
9 by or through the active or passive use of an Inter-
10 net connection, regardless of the medium by or
11 through which that connection is established.

12 (9) ONLINE.—The term “online” refers to any
13 activity regulated by this Act or by section 2710 of
14 title 18, United States Code, that is effected by ac-
15 tive or passive use of an Internet connection, regard-
16 less of the medium by or through which that connec-
17 tion is established.

○