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. INOUYE, 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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Consumer Privacy Protection Act''.

SEC. 2. FINDINGS.

The Congress makes the following findings:

(1) The right to privacy is a personal and fundamental right worthy of protection through appropriate legislation.

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

(3) Existing State, local, and Federal laws provide virtually no privacy protection for Internet users.

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

(5) The Federal Government thus far has eschewed general Internet privacy laws in favor of industry self-regulation, which has led to several self-policing schemes, none of which are enforceable in any meaningful way or provide sufficient consumer protection.

(6) State governments have been reluctant to enter the field of Internet privacy regulation because use of the Internet often crosses State, or even national, boundaries.

(7) States are nonetheless interested in providing greater privacy protection to their citizens as

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

(8) Personal information flowing over the Internet requires greater privacy protection than is currently available today. Vast amounts of personal information about individual Internet users are collected on the Internet and sold or otherwise transferred to third parties.

(9) Poll after poll consistently demonstrates that individual Internet users are highly troubled over their lack of control over their personal information.

(10) Research on the Internet industry demonstrates that consumer concerns about their privacy on the Internet has a correlative negative impact on the development of e-commerce.

(11) Notwithstanding these concerns, the Internet is becoming a major part of the personal and commercial lives of millions of Americans, providing increased access to information, as well as communications and commercial opportunities.

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

vacy is fully protected on our Nation's telecommunications networks and on the Internet.

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

(14) Absent the recognition of these rights and the establishment of consequent industry responsibilities to safeguard those rights, consumer privacy will soon be more gravely threatened.

(15) The ease of gathering and compiling personal information on the Internet, both overtly and surreptitiously, is becoming increasingly efficient and effortless due to advances in digital communications technology which have provided information gatherers the ability to seamlessly compile highly detailed personal histories of Internet users.

(16) Consumers must have—

(A) clear and conspicuous notice that information is being collected about them;

(B) clear and conspicuous notice as to the information gatherer's intent with respect to that information;

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

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

(17) Fair information practices include providing consumers with knowledge of any data collection clear and conspicuous notice of an entity's information practices, the ability to control whether or not those practices will be applied to them personally, access to information collected about them, and safeguards to ensure the integrity and security of that information.

(18) Recent surveys of websites conducted by the Federal Trade Commission and Georgetown University found that a small minority of websites surveyed contained a privacy policy embodying fair information practices such as notice, choice, access, and security.

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

(20) Consumer privacy with respect to written materials, music, and movies should be protected vigilantly to ensure the free exercise of First Amendment rights of expression, regardless of medium.

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

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

(23) In light of the convergence of and emerging competition among and between wireless, wireline, satellite, broadcast, and cable companies, privacy safeguards should be applied uniformly across different communications media so as to provide consistent consumer privacy protections as well as a level competitive playing field for industry.

(24) Notwithstanding the recent focus on Internet privacy, privacy issues abound in the traditional, or offline, marketplace that merit Federal attention.

(25) The Congress would benefit from an exhaustive analysis of general marketplace privacy issues conducted by the agency with the most expertise in this area, the Federal Trade Commission.

(26) While American workers are growing increasingly concerned that their employers may be

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

(27) While employers may have a legitimate need to maintain an efficient and productive workforce, that need should not improperly impinge on employee privacy rights in the workplace.

(28) Databases containing personal information about consumers' commercial purchasing, browsing, and shopping habits, as well as their generalized product preferences, represent considerable commercial value.

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

SEC. 3. PREEMPTION OF INCONSISTENT STATE LAW OR REGULATIONS.

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

(b) EXCEPTIONS.—

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

(A) the law of torts in any State;

(B) the common law in any State; or

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

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

SEC. 4. TABLE OF CONTENTS.

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 IDENTIFIABLE 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.

TITLE I—ONLINE PRIVACY

SEC. 101. COLLECTION OR DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION.

An Internet service provider, online service provider, or operator of a commercial website on the Internet may not collect, use, or disclose personally identifiable information about a user of that service or website except in accordance with the provisions of this title.

SEC. 102. NOTICE, CONSENT, ACCESS, AND SECURITY REQUIREMENTS.

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

calculated to provide actual notice to any user or prospective user that personally identifiable information may be collected from that user. The notice shall disclose—

(1) the specific information that will be collected;

(2) the methods of collecting and using the information collected; and

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

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

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

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

unless the provider or operator obtains that user's affirmative consent, in advance, to the collection and disclosure or use of that information.

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

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

(2) provide a reasonable opportunity for a user to correct, delete, or supplement any such information maintained by that provider or operator; and

(3) make the correction or supplementary information a part of that user's personally identifiable information for all future disclosure and other use purposes.

(d) SECURITY.—An Internet service provider, online service provider, or operator of a commercial website shall establish and maintain reasonable procedures necessary to protect the security, confidentiality, and integrity of personally identifiable information maintained by that provider or operator.

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

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

(2) may not collect, disclose, or otherwise use any personally identifiable information in accordance with the changed policy unless the user has affirmatively consented, under subsection (b), to its collection, disclosure, or use in accordance with the changed policy.

(f) NOTICE OF PRIVACY BREACH.—

(1) IN GENERAL.—If an Internet service provider, online service provider, or operator of a commercial website commits a breach of privacy with respect to the personally identifiable information of a user, then it shall, as soon as reasonably possible, notify all users whose personally identifiable information was affected by that breach. The notice shall describe the nature of the breach and the steps taken by the provider or operator to remedy it.

(2) BREACH OF PRIVACY.—For purposes of paragraph (1), an Internet service provider, online service provider, or operator of a commercial website commits a breach of privacy with respect to personally identifiable information of a user if—

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

(B) it knows that the security, confidentiality, or integrity of personally identifiable information is compromised by any act or failure to act on the part of the provider or operator or by any function of the Internet service or online service provided, or commercial website operated, by that provider or operator that resulted in a disclosure, or possible disclosure, of that information.

(g) APPLICATION TO CERTAIN THIRD-PARTY OPERATORS.—The provisions of this section applicable to Internet service providers, online service providers, and commercial website operators apply to any third party, including an advertiser, that uses that service or website to collect information about users of that service or website.

SEC. 103. OTHER KINDS OF INFORMATION.

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

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

(1) collect information described in subsection (a) from a user of that service or website, or

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

unless the provider or operator obtains that user's consent to the collection and disclosure or other use of that information. For purposes of this subsection, the user will be deemed to have consented unless the user objects to the collection and disclosure or other use of the information.

(c) APPLICATION TO CERTAIN THIRD-PARTY OPERATORS.—The provisions of this section applicable to Internet service providers, online service providers, and commercial website operators apply to any third party, including an advertiser, that uses that service or website to collect information about users of that service or website.

SEC. 104. EXCEPTIONS.

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

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

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

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

SEC. 105. PERMANENCE OF CONSENT.

The consent or denial of consent by a user of permission to an Internet service provider, online service provider, or operator of a commercial website to collect, disclose, or otherwise use any information about that user for which consent is required under this title—

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

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

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

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

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

(a) IN GENERAL.—Notwithstanding any other provision of this title, an Internet service provider, online service provider, operator of a commercial website, or third party that uses such a service or website to collect information about users of that service or website may disclose personally identifiable information about a user of that service or website—

(1) to a law enforcement agency in response to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, or a court order issued in accordance with subsection (c); and

(2) in response to a court order in a civil proceeding granted upon a showing of compelling need

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

(A) the user to whom the information relates is given reasonable notice by the person seeking the information of the court proceeding at which the order is requested; and

(B) that user is afforded a reasonable opportunity to appear and contest the issuance of requested order or to narrow its scope.

(b) SAFEGUARDS AGAINST FURTHER DISCLOSURE.—A court that issues an order described in subsection (a) shall impose appropriate safeguards on the use of the information to protect against its unauthorized disclosure.

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

online service provider, or operator of the commercial website, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on the provider or operator.

SEC. 107. EFFECTIVE DATE.

(a) IN GENERAL.—This title takes effect after the Federal Trade Commission completes the rulemaking procedure under section 109.

(b) APPLICATION TO PRE-EXISTING DATA.—

(1) IN GENERAL.—After the effective date of this title, and except as provided in paragraphs (2) and (3), sections 101, 102, and 103 apply to information collected before the date of enactment of this Act.

(2) COLLECTION OF BOTH KINDS OF INFORMATION.—Section 102(b)(1) and 103(b)(1) do not apply to information collected before the effective date of this title.

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

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

SEC. 108. FTC RULEMAKING PROCEDURE REQUIRED.

The Federal Trade Commission shall initiate a rulemaking procedure within 90 days after the date of enactment of this Act to implement the provisions of this title. Notwithstanding any requirement of chapter 5 of title 5, United States Code, the Commission shall complete the rulemaking procedure not later than 270 days after it is commenced.

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

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

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

"§ 2710. Wrongful disclosure of information about video, book, or recorded music rental, sale, or delivery

''(a) DEFINITIONS.—In this section:

''(1) The term 'book dealer' means any person engaged in the business, in or affecting interstate or foreign commerce, of renting, selling, or delivering books, magazines, or other written or printed material (regardless of the format or medium), or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

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

''(3) The term 'consumer' means any renter, purchaser, or user of goods or services from a video provider, book dealer, or recorded music dealer.

''(4) The term 'ordinary course of business' means only debt-collection activities, order fulfillment, request processing, and the transfer of ownership.

''(5) The term 'personally identifiable information' means information that identifies a person as having requested or obtained specific video materials or services, specific books, magazines, or other written or printed materials, or specific recorded music.

''(6) The term 'video provider' means any person engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of recorded videos, regardless of the format in which, or medium on which they are recorded, or similar audio-visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure.

''(b) VIDEO, BOOK, OR RECORDED MUSIC RENTAL, SALE, OR DELIVERY.—

''(1) IN GENERAL.—A video provider, book dealer, or recorded music dealer who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider or seller, as the case may be, shall be liable to the aggrieved person for the relief provided in subsection (d).

''(2) DISCLOSURE.—A video provider, book dealer, or recorded music dealer may disclose personally identifiable information concerning any consumer—

''(A) to the consumer;

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

''(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, or a court order issued in accordance with paragraph (4);

''(D) to any person if the disclosure is solely of the names and addresses of consumers and if—

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

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

books, magazines, or other printed material, or recorded music;

''(E) to any person if the disclosure is incident to the ordinary course of business of the video provider, book dealer, or recorded music dealer; or

''(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if—

''(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

''(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

''(3) SAFEGUARDS.—If an order is granted pursuant to subparagraph (C) or (F) of paragraph (2), the court shall impose appropriate safeguards against unauthorized disclosure.

''(4) COURT ORDERS.—A court order authorizing disclosure under paragraph (2)(C) shall issue only with prior notice to the consumer and only if the law enforcement agency shows that there is

probable cause to believe that a person has engaged, is engaging, or is about to engage in criminal activity and that the records or other information sought are material to the investigation of such activity. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this subsection, on a motion made promptly by the video provider, book dealer, or recorded music dealer, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such video provider, book dealer, or recorded music dealer, as the case may be.''.

(b) CONFORMING AMENDMENTS.—

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

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

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

SEC. 202. EFFECTIVE DATE.

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

TITLE III—ENFORCEMENT AND REMEDIES

SEC. 301. ENFORCEMENT.

Except as provided in section 302(b) and section 2710(d) of title 18, United States Code, this Act shall be enforced by the Federal Trade Commission. Except as otherwise provided in this Act, a violation of this Act may be punished in the same manner as a violation of a regulation of the Federal Trade Commission.

SEC. 302. VIOLATION IS UNFAIR OR DECEPTIVE ACT OR PRACTICE.

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

(b) ENFORCEMENT BY CERTAIN OTHER AGENCIES.—Compliance with title I of this Act shall be enforced under—

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

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

(B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25(a) of the Federal Reserve Act (12 U.S.C. 601 et seq. and 611 et seq.), by the Board; and

(C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System) and insured State branches of foreign banks, by the Board of Directors of the Federal Deposit Insurance Corporation;

(2) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), by the Director of the Office of Thrift Supervision, in the case of a savings association the deposits of which are insured by the Federal Deposit Insurance Corporation;

(3) the Federal Credit Union Act (12 U.S.C. 1751 et seq.) by the National Credit Union Administration Board with respect to any Federal credit union;

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

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

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

(c) EXERCISE OF CERTAIN POWERS.—For the purpose of the exercise by any agency referred to in subsection (b) of its powers under any Act referred to in that subsection, a violation of title I is deemed to be a violation of a requirement imposed under that Act. In addition to its powers under any provision of law specifically referred to in subsection (b), each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under title I of this Act, any other authority conferred on it by law.

(d) ACTIONS BY THE COMMISSION.—The Commission shall prevent any person from violating title I in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any entity that violates any provision of that title is subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act in the same manner, by the same means, and with the same jurisdiction, power, and duties as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of that title.

(e) EFFECT ON OTHER LAWS.—

(1) PRESERVATION OF COMMISSION AUTHORITY.—Nothing contained in this title shall be construed to limit the authority of the Commission under any other provision of law.

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

SEC. 303. PRIVATE RIGHT OF ACTION.

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

(1) an action to enjoin or restrain such violation;

(2) an action to recover for actual monetary loss from such a violation, or to receive $5,000 in damages for each such violation, whichever is greater; or

(3) both such actions.

(b) WILLFUL AND KNOWING VIOLATIONS.—If the court finds that the defendant willfully or knowingly violated title I, the court may, in its discretion, increase the amount of the award available under subsection (a)(2) to $50,000.

(c) EXCEPTION.—Neither an action to enjoin or restrain a violation, nor an action to recover for loss or damage, may be brought under this section for the accidental disclosure of information if the disclosure was caused by an Act of God, network or systems failure, or other event beyond the control of the Internet service provider, online service provider, or operator of a commercial website if

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

(d) ATTORNEYS FEES; PUNITIVE DAMAGES.—Notwithstanding subsection (a)(2), the court in an action brought under this section, may award reasonable attorneys fees and punitive damages to the prevailing party.

SEC. 304. ACTIONS BY STATES.

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates title I, the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to—

(A) enjoin that practice;

(B) enforce compliance with the rule;

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

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

(2) NOTICE.—

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

(i) written notice of that action; and

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

(B) EXEMPTION.—

(i) IN GENERAL.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general determines that it is not feasible to provide the notice described in that subparagraph before the filing of the action.

(ii) NOTIFICATION.—In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Commission at the same time as the attorney general files the action.

(b) INTERVENTION.—

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

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

(2) EFFECT OF INTERVENTION.—If the Commission intervenes in an action under subsection (a), it shall have the right—

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

(B) to file a petition for appeal.

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

(1) conduct investigations;

(2) administer oaths or affirmations; or

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

(d) ACTIONS BY THE COMMISSION.—In any case in which an action is instituted by or on behalf of the Commission for violation of title I, no State may, during the pendency of that action, institute an action under subsection (a) against any defendant named in the complaint in that action for violation of that rule.

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

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

(A) is an inhabitant; or

(B) may be found.

SEC. 305. WHISTLEBLOWER PROTECTION.

(a) IN GENERAL.—No Internet service provider, online service provider, or commercial website operator may discharge or otherwise discriminate against any employee with respect to compensation, terms, conditions, or privileges of employment because the employee (or any person acting pursuant to the request of the employee) provided information to any Federal or State agency or to the Attorney General of the United States or of any State regarding a possible violation of any provision of title I.

(b) ENFORCEMENT.—Any employee or former employee who believes he has been discharged or discriminated against in violation of subsection (a) may file a civil action in the appropriate United States district court before the close of the 2-year period beginning on the date

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

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

(1) to reinstate the employee to his former position;

(2) to pay compensatory damages; or

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

(d) ATTORNEYS FEES; PUNITIVE DAMAGES.—Notwithstanding subsection (c)(2), the court in an action brought under this section, may award reasonable attorneys fees and punitive damages to the prevailing party.

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

(1) deliberately causes or participates in the alleged violation; or

(2) knowingly or recklessly provides substantially false information to such an agency or the Attorney General.

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

SEC. 306. NO EFFECT ON OTHER REMEDIES.

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

SEC. 307. FTC OFFICE OF ONLINE PRIVACY.

The Federal Trade Commission shall establish an Office of Online Privacy headed by a senior level position officer who reports directly to the Commission and its General Counsel. The Office shall study privacy issues associated with electronic commerce and the Internet, the operation of this Act and the effectiveness of the privacy protections provided by title I. The Office shall report its findings and recommendations from time to time to the Commission, and, notwithstanding any law, regulation, or executive order to the contrary, shall submit an annual report directly to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Commerce on the status of online and Internet privacy issues, together with any recommendations for additional legislation relating to those issues.

TITLE IV—COMMUNICATIONS TECHNOLOGY PRIVACY PROTECTIONS

SEC. 401. PRIVACY PROTECTION FOR SUBSCRIBERS OF SATELLITE TELEVISION SERVICES FOR PRIVATE HOME VIEWING.

(a) IN GENERAL.—Section 631 of the Communications Act of 1934 (47 U.S.C. 551) is amended to read as follows:

"SEC. 631. PRIVACY OF SUBSCRIBER INFORMATION FOR SUBSCRIBERS OF CABLE SERVICE AND SATELLITE TELEVISION SERVICE.

''(a) NOTICE TO SUBSCRIBERS REGARDING PERSONALLY IDENTIFIABLE INFORMATION.—At the time of entering into an agreement to provide any cable service, satellite home viewing service, or other service to a subscriber, and not less often than annually thereafter, a cable operator, satellite carrier, or distributor shall provide notice in the form of a separate, written statement to such subscriber that clearly and conspicuously informs the subscriber of—

''(1) the nature of personally identifiable information collected or to be collected with respect to the subscriber as a result of the provision of such

service and the nature of the use of such information;

''(2) the nature, frequency, and purpose of any disclosure that may be made of such information, including an identification of the types of persons to whom the disclosure may be made;

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

''(4) the times and place at which the subscriber may have access to such information in accordance with subsection (d); and

''(5) the limitations provided by this section with respect to the collection and disclosure of information by the cable operator, satellite carrier, or distributor and the right of the subscriber under this section to enforce such limitations.

''(b) COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION.—

''(1) IN GENERAL.—Except as provided in paragraph (2), a cable operator, satellite carrier, or distributor shall not use its cable or satellite system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber.

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

''(A) obtain information necessary to render a cable or satellite service or other service provided by the cable operator, satellite carrier, or distributor to the subscriber; or

''(B) detect unauthorized reception of cable or satellite communications.

''(c) DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION.—

''(1) IN GENERAL.—Except as provided in paragraph (2), a cable operator, satellite carrier, or distributor may not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or the cable operator, satellite carrier, or distributor.

''(2) EXCEPTIONS.—A cable operator, satellite carrier, or distributor may disclose information described in paragraph (1) if the disclosure is—

''(A) necessary to render, or conduct a legitimate business activity related to, a cable or satellite service or other service provided by the cable operator, satellite carrier, or distributor to the subscriber;

''(B) subject to paragraph (3), made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed; or

''(C) a disclosure of the names and addresses of subscribers to any other provider of cable or satellite service or other service, if—

''(i) the cable operator, satellite carrier, or distributor has provided the subscriber the opportunity to prohibit or limit such disclosure; and

''(ii) the disclosure does not reveal, directly or indirectly—

''(I) the extent of any viewing or other use by the subscriber of a cable or satellite service or other service provided by the cable operator, satellite carrier, or distributor; or

''(II) the nature of any transaction made by the subscriber over

the cable or satellite system of the cable operator, satellite carrier, or distributor.

''(3) COURT ORDERS.—A governmental entity may obtain personally identifiable information concerning a cable or satellite subscriber pursuant to a court order only if, in the court proceeding relevant to such court order—

''(A) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and

''(B) the subject of the information is afforded the opportunity to appear and contest such entity's claim.

''(d) SUBSCRIBER ACCESS TO INFORMATION.—A cable or satellite subscriber shall be provided access to all personally identifiable information regarding that subscriber that is collected and maintained by a cable operator, satellite carrier, or distributor. Such information shall be made available to the subscriber at reasonable times and at a convenient place designated by such cable operator, satellite carrier, or distributor. A cable or sat-

ellite subscriber shall be provided reasonable opportunity to correct any error in such information.

''(e) DESTRUCTION OF INFORMATION.—A cable operator, satellite carrier, or distributor shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (d) or pursuant to a court order.

''(f) RELIEF.—

''(1) IN GENERAL.—Any person aggrieved by any act of a cable operator, satellite carrier, or distributor in violation of this section may bring a civil action in a district court of the United States.

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

''(A) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is greater;

''(B) punitive damages; and

''(C) reasonable attorneys' fees and other litigation costs reasonably incurred.

''(3) NO EFFECT ON OTHER REMEDIES.—The remedy provided by this subsection shall be in addition to any other remedy available under any provision of law to a cable or satellite subscriber.

''(g) DEFINITIONS.—In this section:

''(1) DISTRIBUTOR.—The term 'distributor' means an entity that contracts to distribute secondary transmissions from a satellite carrier and, either as a single channel or in a package with other programming, provides the secondary transmission either directly to individual subscribers for private home viewing or indirectly through other program distribution entities.

''(2) CABLE OPERATOR.—

''(A) IN GENERAL.—The term 'cable operator' has the meaning given that term in section 602.

''(B) INCLUSION.—The term includes any person who—

''(i) is owned or controlled by, or under common ownership or control with, a cable operator; and

''(ii) provides any wire or radio communications service.

''(3) OTHER SERVICE.—The term 'other service' includes any wire, electronic, or radio communications service provided using any of the facilities of a cable operator, satellite carrier, or distributor that are used in the provision of cable service or satellite home viewing service.

''(4) PERSONALLY IDENTIFIABLE INFORMATION.—The term 'personally identifiable information' does not include any record of aggregate data that does not identify particular persons.

''(5) SATELLITE CARRIER.—The term 'satellite carrier' means an entity that uses the facilities of a satellite or satellite service licensed by the Federal Communications Commission and operates in the Fixed-Satellite Service under part 25 of title 47 of the Code of Federal Regulations or the Direct Broadcast Satellite Service under part 100 of title 47 of the Code of Federal Regulations, to establish and operate a channel of communications for point-to-multipoint distribution of television station signals, and that owns or leases a capacity or service on a satellite in order to provide such point-to-multipoint distribution, except to the extent that such entity provides such distribution pursuant to

tariff under the Communications Act of 1934, other than for private home viewing.''.

(b) NOTICE WITH RESPECT TO CERTAIN AGREEMENTS.—

(1) IN GENERAL.—Except as provided in paragraph (2), a cable operator, satellite carrier, or distributor who has entered into agreements referred to in section 631(a) of the Communications Act of 1934, as amended by subsection (a), before the date of enactment of this Act, shall provide any notice required under that section, as so amended, to subscribers under such agreements not later than 180 days after that date.

(2) EXCEPTION.—Paragraph (1) shall not apply with respect to any agreement under which a cable operator, satellite carrier, or distributor was providing notice under section 631(a) of the Communications Act of 1934, as in effect on the day before the date of enactment of this Act, as of such date.

SEC. 402. CUSTOMER PROPRIETARY NETWORK INFORMATION.

Section 222 (c)(1) of the Communications Act of 1934 (47 U.S.C. 222 (c)(1)) is amended by striking ''approval'' and inserting ''express prior authorization''.

TITLE V—RULEMAKING AND STUDIES

SEC. 501. FEDERAL TRADE COMMISSION EXAMINATION.

(a) PROCEEDING REQUIRED.—The Federal Trade Commission shall—

(1) study consumer privacy issues in the traditional, offline marketplace, including whether—

(A) consumers are able, and, if not, the methods by which consumers may be enabled—

(i) to have knowledge that consumer information is being collected about them through their utilization of various offline services and systems;

(ii) to have clear and conspicuous notice that such information could be used, or is intended to be used, by the entity collecting the data for reasons unrelated to the original communications, or that such information could be sold, rented, shared, or otherwise disclosed (or is intended to be sold rented, shared, or otherwise disclosed) to other companies or entities; and

(iii) to stop the reuse, disclosure, or sale of that information;

(B) in the case of consumers who are children, the abilities described in clauses (i), (ii), and (iii) of subparagraph (A) are or can be exercised by their parents; and

(C) changes in the Commission's regulations could provide greater assurance of the offline privacy rights and remedies of parents and consumers generally;

(2) review responses and suggestions from affected commercial and nonprofit entities to changes proposed under paragraph (1)(C); and

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

(b) SCHEDULE FOR FEDERAL TRADE COMMISSION RESPONSES.—The Federal Trade Commission shall, within 6 months after the date of enactment of this Act, submit to Congress a report containing the recommendations required by subsection (a)(3).

SEC. 502. FEDERAL COMMUNICATIONS COMMISSION RULEMAKING.

(a) PROCEEDING REQUIRED.—The Federal Communications Commission shall initiate a rulemaking proceeding to establish uniform consumer privacy rules for

all communications providers. The rulemaking proceeding shall—

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

(2) determine whether consumers are able, and, if not, the methods by which consumers may be enabled to exercise such rights and remedies; and

(3) change the Commission's regulations to coordinate, rationalize, and harmonize laws and regulations administered by the Commission that relate to those rights and remedies.

(b) DEADLINE FOR CHANGES.—The Federal Communications Commission shall complete the rulemaking within 6 months after the date of enactment of this Act.

SEC. 503. DEPARTMENT OF LABOR STUDY OF EMPLOYEE-MONITORING ACTIVITIES.

The Secretary of Labor shall study the extent and nature of employer practices that involving monitoring employee activities both at the workplace and away from the workplace, by electronic or other remote means, including surveillance of electronic mail and Internet use, to determine whether and to what extent such practices constitute an inappropriate violation of employee privacy. The Sec-

retary shall report the results of the study, including findings and recommendations, if any, for legislation or regulation to the Congress within 6 months after the date of enactment of this Act.

TITLE VI—PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION IN BANKRUPTCY

SEC. 601. PERSONALLY IDENTIFIABLE INFORMATION NOT ASSET IN BANKRUPTCY.

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

(1) by striking ''or'' after the semicolon in paragraph (4)(B)(ii);

(2) by striking ''prohibition.'' in paragraph (5) and inserting ''prohibition; or''; and

(3) by inserting after paragraph (5) the following:

''(6) any personally identifiable information (as defined in section 901(6) of the Consumer Privacy Protection Act), or any compilation, or record (in electronic or any other form) of such information.''.

TITLE VII—INTERNET SECURITY INITIATIVES

SEC. 701. FINDINGS.

The Congress finds the following:

(1) Good computer security practices are an underpinning of any privacy protection. The operator of a computer system should protect that system from unauthorized use and secure any private, personal information.

(2) The Federal Government should be a role model in securing its computer systems and should ensure the protection of private, personal information controlled by Federal agencies.

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

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

(5) Some commercial off-the-shelf hardware and off-the-shelf software components to protect computer systems are widely available. There is still a need for long-term computer security research, particularly in the area of infrastructure protection.

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

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

SEC. 702. COMPUTER SECURITY PARTNERSHIP COUNCIL.

(a) ESTABLISHMENT.—The Secretary of Commerce, in consultation with the President's Information Technology Advisory Committee established by Executive Order No. 13035 of February 11, 1997 (62 F.R. 7231), shall establish a 25-member Computer Security Partnership Council.

(b) CHAIRMAN; MEMBERSHIP.—The Council shall have a chairman, appointed by the Secretary, and 24 additional members, appointed by the Secretary as follows:

(1) 5 members, who are not officers or employees of the United States, who are recognized as leaders in the networking and computer security business, at least 1 of whom represents a small or medium-sized company.

(2) 5 members, who are—

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

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

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

(3) 5 members, who are not officers or employees of the United States, who represent public interest groups or State or local governments, of whom at least 2 represent such groups and at least 2 represent such governments.

(4) 5 members, who are not officers or employees of the United States, affiliated with a college, university, or other academic, research-oriented, or public policy institution, with recognized expertise in the field of networking and computer security, whose primary source of employment is by that college, university, or other institution rather than a business organization involved in the networking and computer security business.

(5) 4 members, who are officers or employees of the United States, with recognized expertise in computer systems management, including computer and network security.

(c) FUNCTION.—The Council shall collect and share information about, and increase public awareness of, information security practices and programs, threats to information security, and responses to those threats.

(d) STUDY.—Within 12 months after the date of enactment of this Act, the Council shall publish a report which evaluates and describes areas of computer security research and development that are not adequately developed or funded.

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

SEC. 703. RESEARCH AND DEVELOPMENT.

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

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

(2) by inserting after subsection (b) the following:

''(c) RESEARCH AND DEVELOPMENT OF PROTECTION TECHNOLOGIES.—

''(1) IN GENERAL.—The Institute shall establish a program at the National Institute of Stand-

ards and Technology to conduct, or to fund the conduct of, research and development of technology and techniques to provide security for advanced communications and computing systems and networks including the Next Generation Internet, the underlying structure of the Internet, and networked computers.

''(2) PURPOSE.—A purpose of the program established under paragraph (1) is to address issues or problems that are not addressed by market-driven, private-sector information security research. This may include research—

''(A) to identify Internet security problems which are not adequately addressed by current security technologies;

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

''(C) to enhance the security and reliability of the underlying Internet infrastructure while minimizing any adverse operational impacts such as speed; and

''(D) to allow networks to become self-healing and provide for better analysis of the state of Internet and infrastructure operations and security.

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

''(4) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Institute to carry out this subsection—

''(A) $50,000,000 for fiscal year 2001;

''(B) $60,000,000 for fiscal year 2002;

''(C) $70,000,000 for fiscal year 2003;

''(D) $80,000,000 for fiscal year 2004;

''(E) $90,000,000 for fiscal year 2005; and

''(F) $100,000,000 for fiscal year 2006.''.

SEC. 704. COMPUTER SECURITY TRAINING PROGRAMS.

(a) IN GENERAL.—The Secretary of Commerce, in consultation with appropriate Federal agencies, shall establish a program to support the training of individuals in computer security, Internet security, and related fields at institutions of higher education located in the United States.

(b) SUPPORT AUTHORIZED.—Under the program established under subsection (a), the Secretary may provide scholarships, loans, and other forms of financial aid to students at institutions of higher education. The Secretary

shall require a recipient of a scholarship under this program to provide a reasonable period of service as an employee of the United States government after graduation as a condition of the scholarship, and may authorize full or partial forgiveness of indebtedness for loans made under this program in exchange for periods of employment by the United States government.

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

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

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

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

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

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

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

SEC. 705. GOVERNMENT INFORMATION SECURITY STANDARDS.

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

(1) by striking ''and'' after the semicolon in paragraph (4);

(2) by redesignating paragraph (5) as paragraph (6); and

(3) by inserting after paragraph (4) the following:

''(5) to provide guidance and assistance to Federal agencies in the protection of interconnected computer systems and to coordinate Federal response efforts related to unauthorized access to Federal computer systems; and''.

(b) FEDERAL COMPUTER SYSTEM SECURITY TRAINING.—Section 5(b) of the Computer Security Act of 1987 (49 U.S.C. 759 note) is amended—

(1) by striking ''and'' at the end of paragraph (1);

(2) by striking the period at the end of paragraph (2) and inserting in lieu thereof ''; and''; and

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

''(3) to include emphasis on protecting the availability of Federal electronic citizen services and protecting sensitive information in Federal databases and Federal computer sites that are accessible through public networks.''.

SEC. 706. RECOGNITION OF QUALITY IN COMPUTER SECURITY PRACTICES.

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

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

(2) by inserting after subsection (c), the following:

''(d) AWARD PROGRAM.—The Institute may establish a program for the recognition of excellence in Federal computer system security practices, including the development of a seal, symbol, mark, or logo that could be displayed on the website maintained by the operator of such a system recognized under the program. In order to be recognized under the program, the operator—

''(1) shall have implemented exemplary processes for the protection of its systems and the information stored on that system;

''(2) shall have met any standard established under subsection (a);

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

''(4) shall meet such other criteria as the Institute may require.''.

SEC. 707. DEVELOPMENT OF AUTOMATED PRIVACY CONTROLS.

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

(1) by redesignating subsection (f) as subsection (g); and

(2) by inserting after subsection (e) the following:

''(f) DEVELOPMENT OF INTERNET PRIVACY PROGRAM.—The Institute shall encourage and support the development of one or more computer programs, protocols, or other software, such as the World Wide Web Consortium's P3P program, capable of being installed on computers, or computer networks, with Internet access that would reflect the user's preferences for protecting personally-identifiable or other sensitive, privacy-related information, and automatically execute the program, once activated, without requiring user intervention.''.

TITLE VIII—CONGRESSIONAL INFORMATION SECURITY STANDARDS

SEC. 801. EXERCISE OF RULEMAKING POWER.

This title is enacted by the Congress—

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

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

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

SEC. 802. SENATE.

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

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

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

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

identifiable information and an opportunity to correct inaccuracies.

(4) SECURITY AND INTEGRITY.—Websites must take reasonable steps to protect the security and integrity of personally identifiable information.

(b) PROCEDURE.—

(1) PROPOSAL.—The Sergeant at Arms shall publish a general notice of proposed rulemaking under section 553(b) of title 5, United States Code, but, instead of publication of a general notice of proposed rulemaking in the Federal Register, the Sergeant at Arms shall transmit such notice to the President pro tempore of the Senate for publication in the Congressional Record on the first day on which the Senate is in session following such transmittal. Such notice shall set forth the recommendations of the Sergeant at Arms for regulations under subsection (a).

(2) COMMENT.—Before adopting regulations, the Sergeant at Arms shall provide a comment period of at least 30 days after publication of general notice of proposed rulemaking.

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

copy of such regulations to the President pro tempore of the Senate for publication in the Congressional Record on the first day on which the Senate is in session following such transmittal.

(c) APPROVAL OF REGULATIONS.—

(1) IN GENERAL.—The regulations adopted by the Sergeant at Arms may be approved by the Senate by resolution.

(2) REFERRAL.—Upon receipt of a notice of adoption of regulations under subsection (b)(3), the presiding officers of the Senate shall refer such notice, together with a copy of such regulations, to the Committee on Rules and Administration of the Senate. The purpose of the referral shall be to consider whether such regulations should be approved.

(3) JOINT REFERRAL AND DISCHARGE.—The presiding officer of the Senate may refer the notice of issuance of regulations, or any resolution of approval of regulations, to one committee or jointly to more than one committee. If a committee of the Senate acts to report a jointly referred measure, any other committee of the Senate must act within 30 calendar days of continuous session, or be automatically discharged.

(4) RESOLUTION OF APPROVAL.—In the case of a resolution of the Senate, the matter after the resolving clause shall be the following: ''the following regulations issued by the Sergeant at Arms on ———— ——, 2——— are hereby approved:'' (the blank spaces being appropriately filled in and the text of the regulations being set forth).

(d) ISSUANCE AND EFFECTIVE DATE.—

(1) PUBLICATION.—After approval of the regulations under subsection (c), the Sergeant at Arms shall submit the regulations to the President pro tempore of the Senate for publication in the Congressional Record on the first day on which the Senate is in session following such transmittal.

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

(3) EFFECTIVE DATE.—The regulations shall become effective not less than 60 days after the regulations are issued, except that the Sergeant at Arms may provide for an earlier effective date for good cause found (within the meaning of section 553(d)(3) of title 5, United States Code) and published with the regulation.

(e) AMENDMENT OF REGULATIONS.—Regulations may be amended in the same manner as is described in this section for the adoption, approval, and issuance of regulations, except that the Sergeant at Arms may dispense with publication of a general notice of proposed rulemaking of minor, technical, or urgent amendments that satisfy the criteria for dispensing with publication of such notice pursuant to section 553(b)(B) of title 5, United States Code.

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

TITLE IX—DEFINITIONS

SEC. 901. DEFINITIONS.

In this Act:

(1) OPERATOR OF A COMMERCIAL WEBSITE.—The term ''operator of a commercial website''—

(A) means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, includ-

ing any person offering products or services for sale through that website or online service, involving commerce—

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

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

(I) another such territory; or

(II) any State or foreign nation; or

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

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

(2) DISCLOSE.—The term ''disclose'' means the release of personally identifiable information about a user of an Internet service, online service, or commercial website by an Internet service provider, online service provider, or operator of a commercial website for any purpose, except where such information is provided to a person who provides support for

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

(3) RELEASE.—The term ''release of personally identifiable information'' means the direct or indirect, active or passive, sharing, selling, renting, or other provision of personally identifiable information of a user of an Internet service, online service, or commercial website to any other person other than the user.

(4) INTERNAL OPERATIONS SUPPORT.—The term ''support for the internal operations of a service or website'' means any activity necessary to maintain the technical functionality of that service or website.

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

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

(B) the use of a chat room, message board, or other online service to gather the information; or

(C) tracking or use of any identifying code linked to a user of such a service or website, including the use of cookies.

(3) COOKIE.—The term ''cookie'' means any program, function, or device, commonly known as a ''cookie'', that makes a record on the user's computer (or other electronic device) of that user's access to an Internet service, online service, or commercial website.

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

(5) INTERNET.—The term ''Internet'' means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio.

(6) PERSONALLY IDENTIFIABLE INFORMATION.—The term ''personally identifiable information'' means individually identifiable information about an individual collected online, including—

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

(B) a home or other physical address including street name and name of a city or town;

(C) an e-mail address;

(D) a telephone number;

(E) a Social Security number;

(F) a credit card number;

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

(H) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or

(I) unique identifying information that an Internet service provider, online service provider, or operator of a commercial website collects and combines with an identifier described in this paragraph.

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

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

(8) OFFLINE.—The term ''offline'' refers to any activity regulated by this Act or by section 2710 of title 18, United States Code, that occurs other than by or through the active or passive use of an Internet connection, regardless of the medium by or through which that connection is established.

(9) ONLINE.—The term ''online'' refers to any activity regulated by this Act or by section 2710 of title 18, United States Code, that is effected by active or passive use of an Internet connection, regardless of the medium by or through which that connection is established.

○