

107TH CONGRESS  
2D SESSION

# S. 2201

To protect the online privacy of individuals who use the Internet.

---

IN THE SENATE OF THE UNITED STATES

APRIL 18, 2002

Mr. HOLLINGS (for himself, Mr. STEVENS, Mr. BURNS, Mr. INOUE, Mr. ROCKEFELLER, Mr. KERRY, Mr. BREAUX, Mrs. CARNAHAN, Mr. CLELAND, and Mr. NELSON of Florida) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation.

---

## A BILL

To protect the online privacy of individuals who use the  
Internet.

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 “Online Personal Pri-  
5 vacy Act”.

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

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

- Sec. 1. Short title.
  - Sec. 2. Table of contents.
  - Sec. 3. Findings.
  - Sec. 4. Preemption of State law or regulations.
- Title I—Online Privacy Protection

- Sec. 101. Collection, use, or disclosure of personally identifiable information.
- Sec. 102. Notice and consent requirements.
- Sec. 103. Policy changes; privacy breach.
- Sec. 104. Exceptions.
- Sec. 105. Access.
- Sec. 106. Security.

Title II—Enforcement

- Sec. 201. Enforcement by Federal Trade Commission.
- Sec. 202. Violation is unfair or deceptive act or practice.
- Sec. 203. Private right of action.
- Sec. 204. Actions by States.
- Sec. 205. Whistleblower protection.
- Sec. 206. No effect on other remedies.

Title III—Application to Congress and Federal Agencies

- Sec. 301. Exercise of rulemaking power.
- Sec. 302. Senate.
- Sec. 303. Application to Federal agencies.

Title IV—Miscellaneous

- Sec. 401. Definitions.
- Sec. 402. Effective date.
- Sec. 403. FTC rulemaking.
- Sec. 404. FTC report.
- Sec. 405. Development of automated privacy controls.

1 **SEC. 3. FINDINGS.**

2 The Congress finds the following:

3 (1) The right to privacy is a personal and fun-  
4 damental right worthy of protection through appro-  
5 priate legislation.

6 (2) Individuals engaging in and interacting with  
7 companies engaged in interstate commerce have a  
8 significant interest in their personal information, as  
9 well as a right to control how that information is  
10 collected, used, or transferred.

11 (3) Absent the recognition of these rights and  
12 the establishment of consequent industry responsibil-  
13 ities to safeguard those rights, the privacy of indi-

1 individuals who use the Internet will soon be more  
2 gravely threatened.

3 (4) To extent that States regulate, their efforts  
4 to address Internet privacy will lead to a patchwork  
5 of inconsistent standards and protections.

6 (5) Existing State, local, and Federal laws pro-  
7 vide minimal privacy protection for Internet users.

8 (6) With the exception of Federal Trade Com-  
9 mission enforcement of laws against unfair and de-  
10 ceptive practices, the Federal Government thus far  
11 has eschewed general Internet privacy laws in favor  
12 of industry self-regulation, which has led to several  
13 self-policing schemes, none of which are enforceable  
14 in any meaningful way or provide sufficient privacy  
15 protection to individuals.

16 (7) State governments have been reluctant to  
17 enter the field of Internet privacy regulation because  
18 use of the Internet often crosses State, or even na-  
19 tional, boundaries.

20 (8) States are nonetheless interested in pro-  
21 viding greater privacy protection to their citizens as  
22 evidenced by recent lawsuits brought against offline  
23 and online companies by State attorneys general to  
24 protect the privacy of individuals using the Internet.

1           (9) The ease of gathering and compiling per-  
2           sonal information on the Internet, both overtly and  
3           surreptitiously, is becoming increasingly efficient  
4           and effortless due to advances in digital communica-  
5           tions technology which have provided information  
6           gatherers the ability to compile seamlessly highly de-  
7           tailed personal histories of Internet users.

8           (10) Personal information flowing over the  
9           Internet requires greater privacy protection than is  
10          currently available today. Vast amounts of personal  
11          information, including sensitive information, about  
12          individual Internet users are collected on the Inter-  
13          net and sold or otherwise transferred to third par-  
14          ties.

15          (11) Poll after poll consistently demonstrates  
16          that individual Internet users are highly troubled  
17          over their lack of control over their personal infor-  
18          mation.

19          (12) Market research demonstrates that tens of  
20          billions of dollars in e-commerce are lost due to indi-  
21          vidual fears about a lack of privacy protection on the  
22          Internet.

23          (13) Market research demonstrates that as  
24          many as one-third of all Internet users give false in-  
25          formation about themselves to protect their privacy,

1       due to fears about a lack of privacy protection on  
2       the Internet.

3           (14) Notwithstanding these concerns, the Inter-  
4       net is becoming a major part of the personal and  
5       commercial lives of millions of Americans, providing  
6       increased access to information, as well as commu-  
7       nications and commercial opportunities.

8           (15) It is important to establish personal pri-  
9       vacy rights and industry obligations now so that in-  
10      dividuals have confidence that their personal privacy  
11      is fully protected on the Internet.

12          (16) The social and economic costs of estab-  
13      lishing baseline privacy standards now will be lower  
14      than if Congress waits until the Internet becomes  
15      more prevalent in our everyday lives in coming  
16      years.

17          (17) Whatever costs may be borne by industry  
18      will be significantly offset by the economic benefits  
19      to the commercial Internet created by increased con-  
20      sumer confidence occasioned by greater privacy pro-  
21      tection.

22          (18) Toward the close of the 20th Century, as  
23      individuals' personal information was increasingly  
24      collected, profiled, and shared for commercial pur-  
25      poses, and as technology advanced to facilitate these

1 practices, the Congress enacted numerous statutes  
2 to protect privacy.

3 (19) Those statutes apply to the government,  
4 telephones, cable television, e-mail, video tape rent-  
5 als, and the Internet (but only with respect to chil-  
6 dren).

7 (20) Those statutes all provide significant pri-  
8 vacy protections, but neither limit technology nor  
9 stifle business.

10 (21) Those statutes ensure that the collection  
11 and commercialization of individuals' personal infor-  
12 mation is fair, transparent, and subject to law.

13 **SEC. 4. PREEMPTION OF STATE LAW OR REGULATIONS.**

14 This Act supersedes any State statute, regulation, or  
15 rule regulating Internet privacy to the extent that it re-  
16 lates to the collection, use, or disclosure of personally iden-  
17 tifiable information obtained through the Internet.

18 **TITLE I—ONLINE PRIVACY**  
19 **PROTECTION**

20 **SEC. 101. COLLECTION, USE, OR DISCLOSURE OF PERSON-**  
21 **ALLY IDENTIFIABLE INFORMATION.**

22 (a) IN GENERAL.—An internet service provider, on-  
23 line service provider, or operator of a commercial website  
24 on the Internet may not collect personally identifiable in-  
25 formation from a user, or use or disclose personally identi-

1 fiable information about a user, of that service or website  
2 except in accordance with the provisions of this Act.

3 (b) APPLICATION TO CERTAIN THIRD-PARTY OPERA-  
4 TORS.—The provisions of this Act applicable to internet  
5 service providers, online service providers, and commercial  
6 website operators apply to any third party, including an  
7 advertising network, that uses an internet service provider,  
8 online service provider, or commercial website operator to  
9 collect information about users of that service or website.

10 **SEC. 102. NOTICE AND CONSENT REQUIREMENTS.**

11 (a) NOTICE.—Except as provided in section 104, an  
12 internet service provider, online service provider, or oper-  
13 ator of a commercial website may not collect personally  
14 identifiable information from a user of that service or  
15 website online unless that provider or operator provides  
16 clear and conspicuous notice to the user in the manner  
17 required by this section for the kind of personally identifi-  
18 able information to be collected. The notice shall  
19 disclose—

20 (1) the specific types of information that will be  
21 collected;

22 (2) the methods of collecting and using the in-  
23 formation collected; and

24 (3) all disclosure practices of that provider or  
25 operator for personally identifiable information so

1 collected, including whether it will be disclosed to  
2 third parties.

3 (b) SENSITIVE PERSONALLY IDENTIFIABLE INFOR-  
4 MATION REQUIRES OPT-IN CONSENT.—An internet serv-  
5 ice provider, online service provider, or operator of a com-  
6 mercial website may not—

7 (1) collect sensitive personally identifiable infor-  
8 mation online, or

9 (2) disclose or otherwise use such information  
10 collected online, from a user of that service or  
11 website,

12 unless the provider or operator obtains that user's affirm-  
13 ative consent to the collection and disclosure or use of that  
14 information before, or at the time, the information is col-  
15 lected.

16 (c) NONSENSITIVE PERSONALLY IDENTIFIABLE IN-  
17 FORMATION REQUIRES ROBUST NOTICE AND OPT-OUT  
18 CONSENT.—An internet service provider, online service  
19 provider, or operator of a commercial website may not—

20 (1) collect personally identifiable information  
21 not described in subsection (b) online, or

22 (2) disclose or otherwise use such information  
23 collected online, from a user of that service or  
24 website,

1 unless the provider or operator provides robust notice to  
2 the user, in addition to clear and conspicuous notice, and  
3 has given the user an opportunity to decline consent for  
4 such collection and use by the provider or operator before,  
5 or at the time, the information is collected.

6 (d) INITIAL NOTICE ONLY FOR ROBUST NOTICE.—

7 An internet service provider, online service provider, or op-  
8 erator of a commercial website shall provide robust notice  
9 under subsection (c) of this section to a user only upon  
10 its first collection of non-sensitive personally identifiable  
11 information from that user, except that a subsequent col-  
12 lection of additional or materially different non-sensitive  
13 personally identifiable information from that user shall be  
14 treated as a first collection of such information from that  
15 user.

16 (e) PERMANENCE OF CONSENT.—

17 (1) IN GENERAL.—The consent or denial of  
18 consent by a user of permission to an internet serv-  
19 ice provider, online service provider, or operator of  
20 a commercial website to collect, disclose, or other-  
21 wise use any information about that user for which  
22 consent is required under this Act—

23 (A) shall remain in effect until changed by  
24 the user; and

1 (B) shall apply to the collection, disclosure,  
2 or other use of that information by any entity  
3 that is a commercial successor of, or legal suc-  
4 cessor-in-interest to, that provider or operator,  
5 without regard to the legal form in which such  
6 succession was accomplished (including any en-  
7 tity that collects, discloses, or uses such infor-  
8 mation as a result of a proceeding under chap-  
9 ter 7 or chapter 11 of title 11, United States  
10 Code, with respect to the provider or operator).

11 (2) EXCEPTION.—The consent by a user to the  
12 collection, disclosure, or other use of information  
13 about that user for which consent is required under  
14 this Act does not apply to the collection, disclosure,  
15 or use of that information by a successor entity  
16 under paragraph (1)(B) if—

17 (A) the kind of information collected by  
18 the successor entity about the user is materially  
19 different from the kind of information collected  
20 by the predecessor entity;

21 (B) the methods of collecting and using  
22 the information employed by the successor enti-  
23 ty are materially different from the methods  
24 employed by the predecessor entity; or

1 (C) the disclosure practices of the suc-  
2 cessor entity are materially different from the  
3 practices of the predecessor entity.

4 **SEC. 103. POLICY CHANGES; BREACH OF PRIVACY.**

5 (a) NOTICE OF POLICY CHANGE.—Whenever an  
6 internet service provider, online service provider, or oper-  
7 ator of a commercial website makes a material change in  
8 its policy for the collection, use, or disclosure of sensitive  
9 or nonsensitive personally identifiable information, it—

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

12 (2) may not collect, disclose, or otherwise use  
13 any sensitive or nonsensitive personally identifiable  
14 information in accordance with the changed policy  
15 unless the user has been afforded an opportunity to  
16 consent, or withhold consent, to its collection, disclo-  
17 sure, or use in accordance with the requirements of  
18 section 102(b) or (c), whichever is applicable.

19 (b) NOTICE OF BREACH OF PRIVACY.—

20 (1) IN GENERAL.—If the sensitive or nonsen-  
21 sitive personally identifiable information of a user of  
22 an internet service provider, online service provider,  
23 or operator of a commercial website—

1 (A) is collected, disclosed, or otherwise  
2 used by the provider or operator in violation of  
3 any provision of this Act, or

4 (B) the security, confidentiality, or integ-  
5 rity of such information is compromised by a  
6 hacker or other third party, or by any act or  
7 failure to act of the provider or operator,

8 then the provider or operator shall notify all users  
9 whose sensitive or nonsensitive personally identifi-  
10 able information was affected by the unlawful collec-  
11 tion, disclosure, use, or compromise. The notice shall  
12 describe the nature of the unlawful collection, disclo-  
13 sure, use, or compromise and the steps taken by the  
14 provider or operator to remedy it.

15 (2) DELAY OF NOTIFICATION.—

16 (A) ACTION TAKEN BY INDIVIDUALS.—If  
17 the compromise of the security, confidentiality,  
18 or integrity of the information is caused by a  
19 hacker or other external interference with the  
20 service or website, or by an employee of the  
21 service or website, the provider or operator may  
22 postpone issuing the notice required by para-  
23 graph (1) for a reasonable period of time in  
24 order to—

1 (i) facilitate the detection and appre-  
2 hension of the person responsible for the  
3 compromise; and

4 (ii) take such measures as may be  
5 necessary to restore the integrity of the  
6 service or website and prevent any further  
7 compromise of the security, confidentiality,  
8 and integrity of such information.

9 (B) SYSTEM FAILURES AND OTHER FUNC-  
10 TIONAL CAUSES.—If the unlawful collection,  
11 disclosure, use, or compromise of the security,  
12 confidentiality, and integrity of the information  
13 is the result of a system failure, a problem with  
14 the operating system, software, or program  
15 used by the internet service provider, online  
16 service provider, or operator of the commercial  
17 website, or other non-external interference with  
18 the service or website, the provider or operator  
19 may postpone issuing the notice required by  
20 paragraph (1) for a reasonable period of time  
21 in order to—

22 (i) restore the system's functionality  
23 or fix the problem; and

24 (ii) take such measures as may be  
25 necessary to restore the integrity of the

1 service or website and prevent any further  
2 compromise of the security, confidentiality,  
3 and integrity of the information after the  
4 failure or problem has been fixed and the  
5 integrity of the service or website has been  
6 restored.

7 **SEC. 104. EXCEPTIONS.**

8 (a) IN GENERAL.—Section 102 does not apply to the  
9 collection, disclosure, or use by an internet service pro-  
10 vider, online service provider, or operator of a commercial  
11 website of information about a user of that service or  
12 website necessary—

13 (1) to protect the security or integrity of the  
14 service or website or to ensure the safety of other  
15 people or property;

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

19 (3) to provide other products and services inte-  
20 grally related to the transaction, service, product, or  
21 arrangement for which the user provided the infor-  
22 mation.

23 (b) PROTECTED DISCLOSURES.—An internet service  
24 provider, online service provider, or operator of a commer-  
25 cial website may not be held liable under this Act, any

1 other Federal law, or any State law for any disclosure  
2 made in good faith and following reasonable procedures  
3 in responding to—

4 (1) a request for disclosure of personal informa-  
5 tion under section 1302(b)(1)(B)(iii) of the Chil-  
6 dren’s Online Privacy Protection Act of 1998 (15  
7 U.S.C. 6501 et seq.) to the parent of a child; or

8 (2) a request for access to, or correction or de-  
9 letion of, personally identifiable information under  
10 section 105 of this Act.

11 (c) DISCLOSURE TO LAW ENFORCEMENT AGENCY OR  
12 UNDER COURT ORDER.—

13 (1) IN GENERAL.—Notwithstanding any other  
14 provision of this Act, an internet service provider,  
15 online service provider, operator of a commercial  
16 website, or third party that uses such a service or  
17 website to collect information about users of that  
18 service or website may disclose personally identifi-  
19 able information about a user of that service or  
20 website—

21 (A) to a law enforcement, investigatory,  
22 national security, or regulatory agency or de-  
23 partment of the United States in response to a  
24 request or demand made under authority grant-  
25 ed to that agency or department, including a

1 warrant issued under the Federal Rules of  
2 Criminal Procedure, an equivalent State war-  
3 rant, a court order, or a properly executed ad-  
4 ministrative compulsory process; and

5 (B) in response to a court order in a civil  
6 proceeding granted upon a showing of compel-  
7 ling need for the information that cannot be ac-  
8 commodated by any other means if—

9 (i) the user to whom the information  
10 relates is given reasonable notice by the  
11 person seeking the information of the court  
12 proceeding at which the order is requested;  
13 and

14 (ii) that user is afforded a reasonable  
15 opportunity to appear and contest the  
16 issuance of requested order or to narrow  
17 its scope.

18 (2) SAFEGUARDS AGAINST FURTHER DISCLO-  
19 SURE.—A court that issues an order described in  
20 paragraph (1) shall impose appropriate safeguards  
21 on the use of the information to protect against its  
22 unauthorized disclosure.

1 **SEC. 105. ACCESS.**

2 (a) IN GENERAL.—An internet service provider, on-  
3 line service provider, or operator of a commercial website  
4 shall—

5 (1) upon request provide reasonable access to a  
6 user to personally identifiable information that the  
7 provider or operator has collected from the user on-  
8 line, or that the provider or operator has combined  
9 with personally identifiable information collected  
10 from the user online after the effective date of this  
11 Act;

12 (2) provide a reasonable opportunity for a user  
13 to suggest a correction or deletion of any such infor-  
14 mation maintained by that provider or operator to  
15 which the user was granted access; and

16 (3) make the correction a part of that user's  
17 sensitive personally identifiable information or non-  
18 sensitive personally identifiable information (which-  
19 ever is appropriate), or make the deletion, for all fu-  
20 ture disclosure and other use purposes.

21 (b) EXCEPTION.—An internet service provider, online  
22 service provider, or operator of a commercial website may  
23 decline to make a suggested correction a part of that  
24 user's sensitive personally identifiable information or non-  
25 sensitive personally identifiable information (whichever is

1 appropriate), or to make a suggested deletion if the pro-  
2 vider or operator—

3 (1) reasonably believes that the suggested cor-  
4 rection or deletion is inaccurate or otherwise inap-  
5 propriate;

6 (2) notifies the user in writing, or in digital or  
7 other electronic form, of the reasons the provider or  
8 operator believes the suggested correction or deletion  
9 is inaccurate or otherwise inappropriate; and

10 (3) provides a reasonable opportunity for the  
11 user to refute the reasons given by the provider or  
12 operator for declining to make the suggested correc-  
13 tion or deletion.

14 (c) REASONABLENESS TEST.—The reasonableness of  
15 the access or opportunity provided under subsection (a)  
16 or (b) by an internet service provider, online service pro-  
17 vider, or operator of a commercial website shall be deter-  
18 mined by taking into account such factors as the sensi-  
19 tivity of the information requested and the burden or ex-  
20 pense on the provider or operator of complying with the  
21 request, correction, or deletion.

22 (d) REASONABLE ACCESS FEE.—

23 (1) IN GENERAL.—An internet service provider,  
24 online service provider, or operator of a commercial

1 website may impose a reasonable charge for access  
2 under subsection (a).

3 (2) AMOUNT.—The amount of the fee shall not  
4 exceed \$3, except that upon request of a user, a pro-  
5 vider or operator shall provide such access without  
6 charge to that user if the user certifies in writing  
7 that the user—

8 (A) is unemployed and intends to apply for  
9 employment in the 60-day period beginning on  
10 the date on which the certification is made;

11 (B) is a recipient of public welfare assist-  
12 ance; or

13 (C) has reason to believe that the incorrect  
14 information is due to fraud.

15 **SEC. 106. SECURITY.**

16 An internet service provider, online service provider,  
17 or operator of a commercial website shall establish and  
18 maintain reasonable procedures necessary to protect the  
19 security, confidentiality, and integrity of personally identi-  
20 fiable information maintained by that provider or oper-  
21 ator.

1           **TITLE II—ENFORCEMENT**

2   **SEC. 201. ENFORCEMENT BY FEDERAL TRADE COMMIS-**  
3                   **SION.**

4           Except as provided in section 202(b) of this Act and  
5 section 2710(d) of title 18, United States Code, this Act  
6 shall be enforced by the Commission.

7   **SEC. 202. VIOLATION IS UNFAIR OR DECEPTIVE ACT OR**  
8                   **PRACTICE.**

9           (a) IN GENERAL.—The violation of any provision of  
10 title I is an unfair or deceptive act or practice proscribed  
11 under section 18(a)(1)(B) of the Federal Trade Commis-  
12 sion Act (15 U.S.C. 57a(a)(1)(B)).

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

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

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

21                           (B) member banks of the Federal Reserve  
22 System (other than national banks), branches  
23 and agencies of foreign banks (other than Fed-  
24 eral branches, Federal agencies, and insured  
25 State branches of foreign banks), commercial

1 lending companies owned or controlled by for-  
2 eign banks, and organizations operating under  
3 section 25 or 25A of the Federal Reserve Act  
4 (12 U.S.C. 601 and 611), by the Board; and

5 (C) banks insured by the Federal Deposit  
6 Insurance Corporation (other than members of  
7 the Federal Reserve System) and insured State  
8 branches of foreign banks, by the Board of Di-  
9 rectors of the Federal Deposit Insurance Cor-  
10 poration;

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

16 (3) the Federal Credit Union Act (12 U.S.C.  
17 1751 et seq.) by the National Credit Union Adminis-  
18 tration Board with respect to any Federal credit  
19 union;

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

24 (5) the Packers and Stockyards Act, 1921 (7  
25 U.S.C. 181 et seq.) (except as provided in section

1 406 of that Act (7 U.S.C. 226, 227)), by the Sec-  
2 retary of Agriculture with respect to any activities  
3 subject to that Act; and

4 (6) the Farm Credit Act of 1971 (12 U.S.C.  
5 2001 et seq.) by the Farm Credit Administration  
6 with respect to any Federal land bank, Federal land  
7 bank association, Federal intermediate credit bank,  
8 or production credit association.

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

19 (d) ACTIONS BY THE COMMISSION.—The Commis-  
20 sion shall prevent any person from violating title I in the  
21 same manner, by the same means, and with the same ju-  
22 risdiction, powers, and duties as though all applicable  
23 terms and provisions of the Federal Trade Commission  
24 Act (15 U.S.C. 41 et seq.) were incorporated into and  
25 made a part of this Act. Any entity that violates any provi-

1 sion of that subtitle is subject to the penalties and entitled  
2 to the privileges and immunities provided in the Federal  
3 Trade Commission Act in the same manner, by the same  
4 means, and with the same jurisdiction, power, and duties  
5 as though all applicable terms and provisions of the Fed-  
6 eral Trade Commission Act were incorporated into and  
7 made a part of that subtitle.

8 (e) DISPOSITION OF CIVIL PENALTIES OBTAINED BY  
9 FTC ENFORCEMENT ACTION INVOLVING NONSENSITIVE  
10 PERSONALLY IDENTIFIABLE INFORMATION.—

11 (1) IN GENERAL.—If a civil penalty is imposed  
12 on an internet service provider, online service pro-  
13 vider, or commercial website operator in an enforce-  
14 ment action brought by the Commission for a viola-  
15 tion of title I with respect to nonsensitive personally  
16 identifiable information of users of the service or  
17 website, the penalty shall be—

18 (A) paid to the Commission;

19 (B) held by the Commission in trust for  
20 distribution under paragraph (2); and

21 (C) distributed in accordance with para-  
22 graph (2).

23 (2) DISTRIBUTION TO USERS.—Under proce-  
24 dures to be established by the Commission, the Com-  
25 mission shall hold any amount received as a civil

1 penalty for violation of title I for a period of not less  
2 than 180 days for distribution under those proce-  
3 dures to users—

4 (A) whose nonsensitive personally identifi-  
5 able information was the subject of the viola-  
6 tion; and

7 (B) who file claims with the Commission  
8 for compensation for loss or damage from the  
9 violation at such time, in such manner, and  
10 containing such information as the Commission  
11 may require.

12 (3) AMOUNT OF PAYMENT.—The amount a user  
13 may receive under paragraph (2)—

14 (i) shall not exceed \$200; and

15 (ii) may be limited by the Commission  
16 as necessary to afford each such user a  
17 reasonable opportunity to secure that  
18 user's appropriate portion of the amount  
19 available for distribution.

20 (4) REMAINDER.—If the amount of any such  
21 penalty held by the Commission exceeds the sum of  
22 the amounts distributed under paragraph (2) attrib-  
23 utable to that penalty, the excess shall be covered  
24 into the Treasury of the United States as miscella-

1 neous receipts no later than 12 months after it was  
2 paid to the Commission.

3 (f) EFFECT ON OTHER LAWS.—

4 (1) PRESERVATION OF COMMISSION AUTHOR-  
5 ITY.—Nothing contained in this subtitle shall be  
6 construed to limit the authority of the Commission  
7 under any other provision of law.

8 (2) RELATION TO TITLE II OF COMMUNICA-  
9 TIONS ACT.—Nothing in title I requires an operator  
10 of a website or online service to take any action that  
11 is inconsistent with the requirements of section 222  
12 of the Communications Act of 1934 (47 U.S.C.  
13 222).

14 (3) RELATION TO TITLE VI OF COMMUNICA-  
15 TIONS ACT.—Section 631 of the Communications  
16 Act of 1934 (47 U.S.C. 551) is amended by adding  
17 at the end the following:

18 “(i) To the extent that the application of any provi-  
19 sion of this title to a cable operator as an internet service  
20 provider, online service provider, or operator of a commer-  
21 cial website (as those terms are defined in section 401 of  
22 the Online Personal Privacy Act) with respect to the provi-  
23 sion of Internet service or online service, or the operation  
24 of a commercial website, conflicts with the application of  
25 any provision of that Act to such provision or operation,

1 the Act shall be applied in lieu of the conflicting provision  
2 of this title.”.

3 **SEC. 203. ACTIONS BY USERS.**

4 (a) PRIVATE RIGHT OF ACTION FOR SENSITIVE PER-  
5 SONALLY IDENTIFIABLE INFORMATION.—If an internet  
6 service provider, online service provider, or commercial  
7 website operator collects, discloses, or uses the sensitive  
8 personally identifiable information of any person or fails  
9 to provide reasonable access to or reasonable security for  
10 such sensitive personally identifiable information in viola-  
11 tion of any provision of title I then that person may bring  
12 an action in a district court of the United States of appro-  
13 priate jurisdiction—

14 (1) to enjoin or restrain a violation of title I or  
15 to obtain other appropriate relief; and

16 (2) upon a showing of actual harm to that per-  
17 son caused by the violation, to recover the greater  
18 of—

19 (A) the actual monetary loss from the vio-  
20 lation; or

21 (B) \$5,000.

22 (b) REPEATED VIOLATIONS.—If the court finds, in  
23 an action brought under subsection (a) to recover dam-  
24 ages, that the defendant repeatedly and knowingly violated  
25 title I, the court may, in its discretion, increase the

1 amount of the award available under subsection (a)(2)(B)  
2 to an amount not in excess of \$100,000.

3 (c) EXCEPTION.—Neither an action to enjoin or re-  
4 strain a violation, nor an action to recover for loss or dam-  
5 age, may be brought under this section for the accidental  
6 disclosure of information if the disclosure was caused by  
7 an Act of God, unforeseeable network or systems failure,  
8 or other event beyond the control of the Internet service  
9 provider, online service provider, or operator of a commer-  
10 cial website.

11 **SEC. 204. ACTIONS BY STATES.**

12 (a) IN GENERAL.—

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

22 (A) to enjoin that practice;

23 (B) to enforce compliance with the rule;

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

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

6 (2) NOTICE.—

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

11 (i) written notice of that action; and

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

14 (B) EXEMPTION.—

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

22 (ii) NOTIFICATION.—In an action de-  
23 scribed in clause (i), the attorney general  
24 of a State shall provide notice and a copy  
25 of the complaint to the Commission at the

1 same time as the attorney general files the  
2 action.

3 (b) INTERVENTION.—

4 (1) IN GENERAL.—On receiving notice under  
5 subsection (a)(2), the Commission shall have the  
6 right to intervene in the action that is the subject  
7 of the notice.

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

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

13 (B) to file a petition for appeal.

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

19 (1) conduct investigations;

20 (2) administer oaths or affirmations; or

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

23 (d) ACTIONS BY THE COMMISSION.—In any case  
24 in which an action is instituted by or on behalf of the  
25 Commission for violation of title I, no State may, during

1 the pendency of that action, institute an action under  
2 subsection (a) against any defendant named in the com-  
3 plaint in that action for violation of that rule.

4 (e) VENUE; SERVICE OF PROCESS.—

5 (1) VENUE.—Any action brought under sub-  
6 section (a) may be brought in the district court of  
7 the United States that meets applicable require-  
8 ments relating to venue under section 1391 of title  
9 28, United States Code.

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

13 (A) is an inhabitant; or

14 (B) may be found.

15 **SEC. 205. WHISTLEBLOWER PROTECTION.**

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

1 (b) ENFORCEMENT.—Any employee or former em-  
2 ployee who believes he has been discharged or discrimi-  
3 nated against in violation of subsection (a) may file a civil  
4 action in the appropriate United States district court be-  
5 fore the close of the 2-year period beginning on the date  
6 of such discharge or discrimination. The complainant shall  
7 also file a copy of the complaint initiating such action with  
8 the appropriate Federal agency.

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

14 (1) to reinstate the employee to his former posi-  
15 tion;

16 (2) to pay compensatory damages; or

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

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

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

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

1 (e) 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. 206. NO EFFECT ON OTHER REMEDIES.**

6 The remedies provided by sections 203 and 204 are  
7 in addition to any other remedy available under any provi-  
8 sion of law.

9 **TITLE III—APPLICATION TO**  
10 **CONGRESS AND FEDERAL**  
11 **AGENCIES**

12 **SEC. 301. SENATE.**

13 The Sergeant at Arms of the United States Senate  
14 shall develop regulations setting forth an information se-  
15 curity and electronic privacy policy governing use of the  
16 Internet by officers and employees of the Senate that  
17 meets the requirements of title I.

18 **SEC. 302. APPLICATION TO FEDERAL AGENCIES.**

19 (a) IN GENERAL.—Except as provided in subsection  
20 (b), this Act applies to each Federal agency that is an  
21 internet service provider or an online service provider, or  
22 that operates a website, to the extent provided by section  
23 2674 of title 28, United States Code.

24 (b) EXCEPTIONS.—This Act does not apply to any  
25 Federal agency to the extent that the application of this

1 Act would compromise law enforcement activities or the  
2 administration of any investigative, security, or safety op-  
3 eration conducted in accordance with Federal law.

4 **TITLE IV—MISCELLANEOUS**

5 **SEC. 401. DEFINITIONS.**

6 In this Act:

7 (1) COLLECT.—The term “collect” means the  
8 gathering of personally identifiable information  
9 about a user of an Internal service, online service, or  
10 commercial website by or on behalf of the provider  
11 or operator of that service or website by any means,  
12 direct or indirect, active or passive, including—

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

17 (B) the use of a chat room, message board,  
18 or other online service to gather the informa-  
19 tion; or

20 (C) tracking or use of any identifying code  
21 linked to a user of such a service or website, in-  
22 cluding the use of cookies or other tracking  
23 technology.

24 (2) COMMISSION.—The term “Commission”  
25 means the Federal Trade Commission.

1           (3) COOKIE.—The term “cookie” means any  
2           program, function, or device, commonly known as a  
3           “cookie”, that makes a record on the user’s com-  
4           puter (or other electronic device) of that user’s ac-  
5           cess to an internet service, online service, or com-  
6           mercial website.

7           (4) DISCLOSE.—The term “disclose” means the  
8           release of personally identifiable information about a  
9           user of an Internet service, online service, or com-  
10          mercial website by an internet service provider, on-  
11          line service provider, or operator of a commercial  
12          website for any purpose, except where such informa-  
13          tion is provided to a person who provides support for  
14          the internal operations of the service or website and  
15          who does not disclose or use that information for  
16          any other purpose.

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

20          (6) INTERNAL OPERATIONS SUPPORT.—The  
21          term “support for the internal operations of a serv-  
22          ice or website” means any activity necessary to  
23          maintain the technical functionality of that service  
24          or website.

1           (7) INTERNET.—The term “Internet” means  
2           collectively the myriad of computer and tele-  
3           communications facilities, including equipment and  
4           operating software, which comprise the inter-  
5           connected world-wide network of networks that em-  
6           ploy the Transmission Control Protocol/Internet  
7           Protocol, or any predecessor or successor protocols  
8           to such protocol, to communicate information of all  
9           kinds by wire or radio.

10           (8) INTERNET SERVICE PROVIDER; ONLINE  
11           SERVICE PROVIDER; WEBSITE.—The Commission  
12           shall by rule define the terms “internet service pro-  
13           vider”, “online service provider”, and “website”, and  
14           shall revise or amend such rule to take into account  
15           changes in technology, practice, or procedure with  
16           respect to the collection of personal information over  
17           the Internet.

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

24           (10) OPERATOR OF A COMMERCIAL WEBSITE.—  
25           The term “operator of a commercial website”—

1 (A) means any person who operates a  
2 website located on the Internet or an online  
3 service and who collects or maintains personal  
4 information from or about the users of or visi-  
5 tors to such website or online service, or on  
6 whose behalf such information is collected or  
7 maintained, where such website or online serv-  
8 ice is operated for commercial purposes, includ-  
9 ing any person offering products or services for  
10 sale through that website or online service, in-  
11 volving commerce—

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

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

17 (I) another such territory; or

18 (II) any State or foreign nation;

19 or

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

22 but

23 (B) does not include any nonprofit entity  
24 that would otherwise be exempt from coverage

1 under section 5 of the Federal Trade Commis-  
2 sion Act (15 U.S.C. 45).

3 (11) PERSONALLY IDENTIFIABLE INFORMA-  
4 TION.—

5 (A) IN GENERAL.—The term “personally  
6 identifiable information” means individually  
7 identifiable information about an individual col-  
8 lected online, including—

9 (i) a first and last name, whether  
10 given at birth or adoption, assumed, or le-  
11 gally changed;

12 (ii) a home or other physical address  
13 including street name and name of a city  
14 or town;

15 (iii) an e-mail address;

16 (iv) a telephone number;

17 (v) a birth certificate number;

18 (vi) any other identifier for which the  
19 Commission finds there is a substantial  
20 likelihood that the identifier would permit  
21 the physical or online contacting of a spe-  
22 cific individual; or

23 (vii) information that an Internet  
24 service provider, online service provider, or  
25 operator of a commercial website collects

1           and combines with an identifier described  
2           in clauses (i) through (vi) of this subpara-  
3           graph.

4           (B) INFERENTIAL INFORMATION EX-  
5           CLUDED.—Information about an individual de-  
6           rived or inferred from data collected online but  
7           not actually collected online is not personally  
8           identifiable information.

9           (12) RELEASE.—The term “release of person-  
10          ally identifiable information” means the direct or in-  
11          direct, sharing, selling, renting, or other provision of  
12          personally identifiable information of a user of an  
13          internet service, online service, or commercial  
14          website to any other person other than the user.

15          (13) ROBUST NOTICE.—The term “robust no-  
16          tice” means actual notice at the point of collection  
17          of the personally identifiable information describing  
18          briefly and succinctly the intent of the Internet serv-  
19          ice provider, online service provider, or operator of  
20          a commercial website to use or disclose that infor-  
21          mation for marketing or other purposes.

22          (14) SENSITIVE FINANCIAL INFORMATION.—  
23          The term “sensitive financial information” means—

24                  (A) the amount of income earned or losses  
25                  suffered by an individual;

1 (B) an individual's account number or bal-  
2 ance information for a savings, checking, money  
3 market, credit card, brokerage, or other finan-  
4 cial services account;

5 (C) the access code, security password, or  
6 similar mechanism that permits access to an in-  
7 dividual's financial services account;

8 (D) an individual's insurance policy infor-  
9 mation, including the existence, premium, face  
10 amount, or coverage limits of an insurance pol-  
11 icy held by or for the benefit of an individual;  
12 or

13 (E) an individual's outstanding credit card,  
14 debt, or loan obligations.

15 (15) SENSITIVE PERSONALLY IDENTIFIABLE IN-  
16 FORMATION.—The term “sensitive personally identi-  
17 fiable information” means personally identifiable in-  
18 formation about an individual's—

19 (A) individually identifiable health infor-  
20 mation (as defined in section 164.501 of title  
21 45, Code of Federal Regulations);

22 (B) race or ethnicity;

23 (C) political party affiliation;

24 (D) religious beliefs;

25 (E) sexual orientation;

1 (F) a Social Security number; or

2 (G) sensitive financial information.

3 **SEC. 402. EFFECTIVE DATE OF TITLE I.**

4 Title I of this Act takes effect on the day after the  
5 date on which the Commission publishes a final rule under  
6 section 403.

7 **SEC. 403. FTC RULEMAKING.**

8 The Commission shall—

9 (1) initiate a rulemaking within 90 days after  
10 the date of enactment of this Act for regulations to  
11 implement the provisions of title I; and

12 (2) complete that rulemaking within 270 days  
13 after initiating it.

14 **SEC. 404. FTC REPORT.**

15 (a) REPORT.—The Commission shall submit a report  
16 to the Senate Committee on Commerce, Science, and  
17 Transportation and the House of Representatives Com-  
18 mittee on Commerce 18 months after the effective date  
19 of title I, and annually thereafter, on—

20 (1) whether this Act is accomplishing the pur-  
21 poses for which it was enacted;

22 (2) whether technology that protects privacy is  
23 being utilized in the marketplace in such a manner  
24 as to facilitate administration of and compliance  
25 with title I;

1           (3) whether additional legislation is required to  
2           accomplish those purposes or improve the admin-  
3           istrability or effectiveness of this Act;

4           (4) whether legislation is appropriate or nec-  
5           essary to regulate the collection, use, and distribu-  
6           tion of personally identifiable information collected  
7           other than via the Internet;

8           (5) whether and how the government might as-  
9           sist industry in developing standard online privacy  
10          notices that substantially comply with the require-  
11          ments of section 102(a);

12          (6) whether and how the creation of a set of  
13          self-regulatory guidelines established by independent  
14          safe harbor organizations and approved by the Com-  
15          mission would facilitate administration of and com-  
16          pliance with title I; and

17          (7) whether additional legislation is necessary  
18          or appropriate to regulate the collection, use, and  
19          disclosure of personally identifiable information col-  
20          lected online before the effective date of title I.

21          (b) FTC NOTICE OF INQUIRY.—The Commission  
22          shall initiate a notice of inquiry within 90 days after the  
23          date of enactment of this Act to request comment on the  
24          matter described in paragraphs (1) through (7) of sub-  
25          section (a).

1 **SEC. 405. 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) is amended—

5 (1) by redesignating subsection (d) as sub-  
6 section (e); and

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

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

○