

[STAFF WORKING DRAFT]

APRIL 4, 2002

107TH CONGRESS
2D SESSION

S. _____

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

IN THE SENATE OF THE UNITED STATES

APRIL —, 2002

Mr. HOLLINGS (for himself and Mr. STEVENS) introduced the following bill;
which was read twice and referred to the Committee on

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-

1 ities to safeguard those rights, the privacy of indi-
2 viduals who use the Internet will soon be more
3 gravely threatened.

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

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

10 (6) The Federal Government thus far has es-
11 chewed general Internet privacy laws in favor of in-
12 dustry self-regulation, which has led to several self-
13 policing schemes, none of which are enforceable in
14 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 provide give
25 false information about themselves to protect their

1 privacy, due to fears about a lack of privacy protec-
2 tion on 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 notice to the user in the manner required by this section
17 for the kind of personally identifiable information to be
18 collected. The notice shall disclose—

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

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

23 (3) all disclosure practices of that provider or
24 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 provides clear and con-
13 spicuous notice to the user and obtains that user’s affirm-
14 ative consent to the collection and disclosure or use of that
15 information before the information is collected.

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 and has given the user an opportunity to decline
3 consent for such collection and use by the provider or op-
4 erator before the information is collected.

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

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

14 (e) PERMANENCE OF CONSENT.—

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

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

23 (B) shall apply to the collection, disclosure,
24 or other use of that information by any entity
25 that is a commercial successor of, or legal suc-

1 cessor-in-interest to, that provider or operator,
2 without regard to the legal form in which such
3 succession was accomplished (including any en-
4 tity that collects, discloses, or uses such infor-
5 mation as a result of a proceeding under chap-
6 ter 7 or chapter 11 of title 11, United States
7 Code, with respect to the provider or operator).

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

14 (A) the kind of information collected by
15 the successor entity about the user is materially
16 different from the kind of information collected
17 by the predecessor entity;

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

22 (C) the disclosure practices of the suc-
23 cessor entity are materially different from the
24 practices of the predecessor entity.

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

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

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

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

16 (b) NOTICE OF BREACH OF PRIVACY.—

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

21 (A) is collected, disclosed, or otherwise
22 used by the provider or operator in violation of
23 any provision of this Act, or

24 (B) the security, confidentiality, or integ-
25 rity of such information is compromised by a

1 hacker or other third party, or by any act or
2 failure to act of the provider or operator,
3 then the provider or operator shall notify all users
4 whose sensitive or nonsensitive personally identifi-
5 able information was affected by the unlawful collec-
6 tion, disclosure, use, or compromise. The notice shall
7 describe the nature of the unlawful collection, disclo-
8 sure, use, or compromise and the steps taken by the
9 provider or operator to remedy it.

10 (2) DELAY OF NOTIFICATION.—

11 (A) EXTERNAL CAUSE.—If the compromise
12 of the security, confidentiality, or integrity of
13 the information is caused by a hacker or other
14 external interference with the service or website,
15 the provider or operator may postpone issuing
16 the notice required by paragraph (1) for a rea-
17 sonable period of time in order to—

18 (i) facilitate the detection and appre-
19 hension of the person responsible for the
20 compromise; and

21 (ii) take such measures as may be
22 necessary to restore the integrity of the
23 service or website and prevent any further
24 compromise of the security, confidentiality,
25 and integrity of such information.

1 (B) INTERNAL CAUSE.—If the unlawful
2 collection, disclosure, use, or compromise of the
3 security, confidentiality, and integrity of the in-
4 formation is the result of a system failure, a
5 problem with the operating system, software, or
6 program used by the internet service provider,
7 online service provider, or operator of the com-
8 mercial website, or other non-external inter-
9 ference with the service or website, the provider
10 or operator may postpone issuing the notice re-
11 quired by paragraph (1) for a reasonable period
12 of time in order to—

13 (i) restore the system’s functionality
14 or fix the problem; and

15 (ii) take such measures as may be
16 necessary to restore the integrity of the
17 service or website and prevent any further
18 compromise of the security, confidentiality,
19 and integrity of the information after the
20 failure or problem has been fixed and the
21 integrity of the service or website has been
22 restored.

23 **SEC. 104. EXCEPTIONS.**

24 (a) IN GENERAL.—Section 102 does not apply to the
25 collection, disclosure, or use by an internet service pro-

1 vider, online service provider, or operator of a commercial
2 website of information about a user of that service or
3 website necessary—

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

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

9 (3) to provide other products and services inte-
10 grally related to the transaction, service, product, or
11 arrangement for which the user provided the infor-
12 mation.

13 (b) DISCLOSURE TO PARENT PROTECTED.—An
14 internet service provider, online service provider, or oper-
15 ator of a commercial website may not be held liable under
16 this Act, any other Federal law, or any State law for any
17 disclosure made in good faith and following reasonable
18 procedures in responding to a request for disclosure of
19 personal information under section 1302(b)(1)(B)(iii) of
20 the Children’s Online Privacy Protection Act of 1998 (15
21 U.S.C. 6501 et seq.) to the parent of a child.

22 (c) DISCLOSURE TO LAW ENFORCEMENT AGENCY OR
23 UNDER COURT ORDER.—

24 (1) IN GENERAL.—Notwithstanding any other
25 provision of this Act, an internet service provider,

1 online service provider, operator of a commercial
2 website, or third party that uses such a service or
3 website to collect information about users of that
4 service or website may disclose personally identifi-
5 able information about a user of that service or
6 website—

7 (A) to a law enforcement agency in re-
8 sponse to a warrant issued under the Federal
9 Rules of Criminal Procedure, an equivalent
10 State warrant, a court order, or pursuant to a
11 properly executed administrative compulsory
12 process; and

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

17 (i) the user to whom the information
18 relates is given reasonable notice by the
19 person seeking the information of the court
20 proceeding at which the order is requested;
21 and

22 (ii) that user is afforded a reasonable
23 opportunity to appear and contest the
24 issuance of requested order or to narrow
25 its scope.

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

6 **SEC. 105. ACCESS.**

7 (a) IN GENERAL.—An internet service provider, on-
8 line service provider, or operator of a commercial website
9 shall—

10 (1) upon request provide reasonable access to a
11 user to personally identifiable information that the
12 provider or operator has collected from the user, or
13 that the provider or operator has combined with per-
14 sonally identifiable information collected from the
15 user after the effective date of this Act;

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

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

1 (b) EXCEPTION.—An internet service provider, online
2 service provider, or operator of a commercial website may
3 decline to make a suggested correction a part of that
4 user’s sensitive personally identifiable information or non-
5 sensitive personally identifiable information (whichever is
6 appropriate), or to make a suggested deletion if the pro-
7 vider or operator—

8 (1) reasonably believes that the suggested cor-
9 rection or deletion is inaccurate or otherwise inap-
10 propriate;

11 (2) notifies the user in writing of the reasons
12 the provider or operator believes the suggested cor-
13 rection or deletion is inaccurate or otherwise inap-
14 propriate; and

15 (3) provides a reasonable opportunity for the
16 user to refute the reasons given by the provider or
17 operator for declining to make the suggested correc-
18 tion or deletion.

19 (c) REASONABLENESS TEST.—The reasonableness of
20 the access or opportunity provided under subsection (a)
21 or (b) by an internet service provider, online service pro-
22 vider, or operator of a commercial website shall be deter-
23 mined by taking into account such factors as the sensi-
24 tivity of the information requested and the burden or ex-

1 pence on the provider or operator of complying with the
2 request, correction, or deletion.

3 (d) REASONABLE ACCESS FEE.—

4 (1) IN GENERAL.—An internet service provider,
5 online service provider, or operator of a commercial
6 website may impose a reasonable charge for access
7 under subsection (a).

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

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

16 (B) is a recipient of public welfare assist-
17 ance; or

18 (C) has reason to believe that the incorrect
19 information is due to fraud.

20 **SEC. 106. SECURITY.**

21 An internet service provider, online service provider,
22 or operator of a commercial website shall establish and
23 maintain reasonable procedures necessary to protect the
24 security, confidentiality, and integrity of personally identi-

1 fiable information maintained by that provider or oper-
2 ator.

3 **TITLE II—ENFORCEMENT**

4 **SEC. 201. ENFORCEMENT BY FEDERAL TRADE COMMIS-**
5 **SION.**

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

9 **SEC. 202. VIOLATION IS UNFAIR OR DECEPTIVE ACT OR**
10 **PRACTICE.**

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

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

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

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

23 (B) member banks of the Federal Reserve
24 System (other than national banks), branches
25 and agencies of foreign banks (other than Fed-

1 eral branches, Federal agencies, and insured
2 State branches of foreign banks), commercial
3 lending companies owned or controlled by for-
4 eign banks, and organizations operating under
5 section 25 or 25A of the Federal Reserve Act
6 (12 U.S.C. 601 and 611), by the Board; and

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

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

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

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

1 (5) the Packers and Stockyards Act, 1921 (7
2 U.S.C. 181 et seq.) (except as provided in section
3 406 of that Act (7 U.S.C. 226, 227)), by the Sec-
4 retary of Agriculture with respect to any activities
5 subject to that Act; and

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

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

21 (d) ACTIONS BY THE COMMISSION.—The Commis-
22 sion shall prevent any person from violating title I in the
23 same manner, by the same means, and with the same ju-
24 risdiction, powers, and duties as though all applicable
25 terms and provisions of the Federal Trade Commission

1 Act (15 U.S.C. 41 et seq.) were incorporated into and
2 made a part of this Act. Any entity that violates any provi-
3 sion of that subtitle is subject to the penalties and entitled
4 to the privileges and immunities provided in the Federal
5 Trade Commission Act in the same manner, by the same
6 means, and with the same jurisdiction, power, and duties
7 as though all applicable terms and provisions of the Fed-
8 eral Trade Commission Act were incorporated into and
9 made a part of that subtitle.

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

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

20 (A) paid to the Commission;

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

23 (C) distributed in accordance with para-
24 graph (2).

1 (2) DISTRIBUTION TO USERS.—Under proce-
2 dures to be established by the Commission, the Com-
3 mission shall hold any amount received as a civil
4 penalty for violation of title I for a period of not less
5 than 180 days for distribution under those proce-
6 dures to users—

7 (A) whose nonsensitive personally identifi-
8 able information was the subject of the viola-
9 tion; and

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

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

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

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

23 (4) REMAINDER.—If the amount of any such
24 penalty held by the Commission exceeds the sum of
25 the amounts distributed under paragraph (2) attrib-

1 utable to that penalty, the excess shall be covered
2 into the Treasury of the United States as miscella-
3 neous receipts no later than 12 months after it was
4 paid to the Commission.

5 (e) EFFECT ON OTHER LAWS.—

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

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

16 **SEC. 203. ACTIONS BY USERS.**

17 (a) PRIVATE RIGHT OF ACTION FOR SENSITIVE PER-
18 SONALLY IDENTIFIABLE INFORMATION.—If an internet
19 service provider, online service provider, or commercial
20 website operator collects, discloses, or uses the sensitive
21 personally identifiable information of any person or fails
22 to provide reasonable access to or reasonable security for
23 such sensitive personally identifiable information in viola-
24 tion of any provision of title I then that person, if other-
25 wise permitted by the laws or rules of court of a State,

1 may bring an action in an appropriate court of that
2 State—

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

5 (2) upon a showing of actual harm to that per-
6 son caused by the violation, to recover the greater
7 of—

8 (A) the actual monetary loss from the vio-
9 lation; or

10 (B) \$5,000.

11 (b) REPEATED VIOLATIONS.—If the court finds, in
12 an action brought under subsection (a) to recover dam-
13 ages, that the defendant repeatedly and knowingly violated
14 title I, the court may, in its discretion, increase the
15 amount of the award available under subsection (a)(2)(B)
16 to an amount not in excess of \$100,000.

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

1 **SEC. 204. ACTIONS BY STATES.**

2 (a) IN GENERAL.—

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

12 (A) to enjoin that practice;

13 (B) to enforce compliance with the rule;

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

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

19 (2) NOTICE.—

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

24 (i) written notice of that action; and

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

1 (B) EXEMPTION.—

2 (i) IN GENERAL.—Subparagraph (A)
3 shall not apply with respect to the filing of
4 an action by an attorney general of a State
5 under this subsection, if the attorney gen-
6 eral determines that it is not feasible to
7 provide the notice described in that sub-
8 paragraph before the filing of the action.

9 (ii) NOTIFICATION.—In an action de-
10 scribed in clause (i), the attorney general
11 of a State shall provide notice and a copy
12 of the complaint to the Commission at the
13 same time as the attorney general files the
14 action.

15 (b) INTERVENTION.—

16 (1) IN GENERAL.—On receiving notice under
17 subsection (a)(2), the Commission shall have the
18 right to intervene in the action that is the subject
19 of the notice.

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

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

25 (B) to file a petition for appeal.

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

- 6 (1) conduct investigations;
7 (2) administer oaths or affirmations; or
8 (3) compel the attendance of witnesses or the
9 production of documentary and other evidence.

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

16 (e) VENUE; SERVICE OF PROCESS.—

17 (1) VENUE.—Any action brought under sub-
18 section (a) may be brought in the district court of
19 the United States that meets applicable require-
20 ments relating to venue under section 1391 of title
21 28, United States Code.

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

25 (A) is an inhabitant; or

1 (B) may be found.

2 **SEC. 205. WHISTLEBLOWER PROTECTION.**

3 (a) IN GENERAL.—No internet service provider, on-
4 line service provider, or commercial website operator may
5 discharge or otherwise discriminate against any employee
6 with respect to compensation, terms, conditions, or privi-
7 leges of employment because the employee (or any person
8 acting pursuant to the request of the employee) provided
9 information to any Federal or State agency or to the At-
10 torney General of the United States or of any State re-
11 garding a possible violation of any provision of title I.

12 (b) ENFORCEMENT.—Any employee or former em-
13 ployee who believes he has been discharged or discrimi-
14 nated against in violation of subsection (a) may file a civil
15 action in the appropriate United States district court be-
16 fore the close of the 2-year period beginning on the date
17 of such discharge or discrimination. The complainant shall
18 also file a copy of the complaint initiating such action with
19 the appropriate Federal agency.

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

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

3 (2) to pay compensatory damages or provide
4 other appropriate relief; or

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

7 (d) **LIMITATION.**—The protections of this section
8 shall not apply to any employee who—

9 (1) deliberately causes or participates in the al-
10 leged violation; or

11 (2) knowingly or recklessly provides substan-
12 tially false information to such an agency or the At-
13 torney General.

14 (e) **BURDENS OF PROOF.**—The legal burdens of proof
15 that prevail under subchapter III of chapter 12 of title
16 5, United States Code (5 U.S.C. 1221 et seq.) shall govern
17 adjudication of protected activities under this section.

18 **SEC. 206. NO EFFECT ON OTHER REMEDIES.**

19 The remedies provided by sections 203 and 204 are
20 in addition to any other remedy available under any provi-
21 sion of law.

1 **TITLE III—APPLICATION TO**
2 **CONGRESS AND FEDERAL**
3 **AGENCIES**

4 **SEC. 301. SENATE.**

5 The Sergeant at Arms of the United States Senate
6 shall develop regulations setting forth an information se-
7 curity and electronic privacy policy governing use of the
8 Internet by officers and employees of the Senate that
9 meets the requirements of title I.

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

11 (a) IN GENERAL.—This Act applies to each Federal
12 agency that is an internet service provider or an online
13 service provider, or that operates a website.

14 (b) EXCEPTIONS.—This Act does not apply to any
15 Federal agency to the extent that the application of this
16 Act would compromise law enforcement activities or the
17 administration of any investigative, security, or safety op-
18 eration conducted in accordance with Federal law.

19 **TITLE IV—MISCELLANEOUS**

20 **SEC. 401. DEFINITIONS.**

21 In this Act:

22 (1) COLLECT.—The term “collect” means the
23 gathering of personally identifiable information
24 about a user of an Internal service, online service, or
25 commercial website by or on behalf of the provider

1 or operator of that service or website by any means,
2 direct or indirect, active or passive, including—

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

7 (B) the use of a chat room, message board,
8 or other online service to gather the informa-
9 tion; or

10 (C) tracking or use of any identifying code
11 linked to a user of such a service or website, in-
12 cluding the use of cookies or other tracking
13 technology.

14 (2) COMMISSION.—The term “Commission”
15 means the Federal Trade Commission.

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

22 (4) DISCLOSE.—The term “disclose” means the
23 release of personally identifiable information about a
24 user of an Internet service, online service, or com-
25 mercial website by an internet service provider, on-

1 line service provider, or operator of a commercial
2 website for any purpose, except where such informa-
3 tion is provided to a person who provides support for
4 the internal operations of the service or website and
5 who does not disclose or use that information for
6 any other purpose.

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

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

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

24 (8) INTERNET SERVICE PROVIDER; ONLINE
25 SERVICE PROVIDER; WEBSITE.—The Commission

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

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

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

15 (A) means any person who operates a
16 website located on the Internet or an online
17 service and who collects or maintains personal
18 information from or about the users of or visi-
19 tors to such website or online service, or on
20 whose behalf such information is collected or
21 maintained, where such website or online serv-
22 ice is operated for commercial purposes, includ-
23 ing any person offering products or services for
24 sale through that website or online service, in-
25 volving commerce—

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

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

6 (I) another such territory; or

7 (II) any State or foreign nation;

8 or

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

11 but

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

16 (11) PERSONALLY IDENTIFIABLE INFORMA-
17 TION.—

18 (A) IN GENERAL.—The term “personally
19 identifiable information” means individually
20 identifiable information about an individual col-
21 lected online, including—

22 (i) a first and last name, whether
23 given at birth or adoption, assumed, or le-
24 gally changed;

1 (ii) a home or other physical address
2 including street name and name of a city
3 or town;

4 (iii) an e-mail address;

5 (iv) a telephone number;

6 (v) a birth certificate number;

7 (vi) any other identifier for which the
8 Commission finds there is a substantial
9 likelihood that the identifier would permit
10 the physical or online contacting of a spe-
11 cific individual; or

12 (vii) information that an Internet
13 service provider, online service provider, or
14 operator of a commercial website collects
15 and combines with an identifier described
16 in clauses (i) through (vi) of this subpara-
17 graph.

18 (B) INFERENTIAL INFORMATION EX-
19 CLUDED.—Information about an individual de-
20 rived or inferred from data collected online but
21 not actually collected online is not personally
22 identifiable information.

23 (12) RELEASE.—The term “release of person-
24 ally identifiable information” means the direct or in-
25 direct, sharing, selling, renting, or other provision of

1 personally identifiable information of a user of an
2 internet service, online service, or commercial
3 website to any other person other than the user.

4 (13) ROBUST NOTICE.—The term “robust no-
5 tice” means actual notice at the point of collection
6 of the personally identifiable information describing
7 briefly and succinctly the intent of the Internet serv-
8 ice provider, online service provider, or operator of
9 a commercial website to use or disclose that infor-
10 mation for marketing or other purposes.

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

13 (A) the amount of income earned or losses
14 suffered by an individual;

15 (B) an individual’s account number or bal-
16 ance information for a savings, checking, money
17 market, credit card, brokerage, or other finan-
18 cial services account;

19 (C) the access code, security password, or
20 similar mechanism that permits access to an in-
21 dividual’s financial services account;

22 (D) an individual’s insurance policy infor-
23 mation, including the existence, premium, face
24 amount, or coverage limits of an insurance pol-

1 icy held by or for the benefit of an individual;

2 or

3 (E) an individual's outstanding credit card,

4 debt, or loan obligations.

5 (15) SENSITIVE PERSONALLY IDENTIFIABLE IN-

6 FORMATION.—The term “sensitive personally identi-

7 fiable information” means personally identifiable in-

8 formation about an individual that includes informa-

9 tion about that individual's—

10 (A) individually identifiable health infor-

11 mation (as defined in section 164.501 of title

12 45, Code of Federal Regulations);

13 (B) race or ethnicity;

14 (C) political party affiliation;

15 (D) religious beliefs;

16 (E) sexual orientation;

17 (F) a Social Security number; or

18 (G) sensitive financial information.

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

20 Title I of this Act takes effect on the day after the

21 date on which the Commission publishes a final rule under

22 section 403.

1 **SEC. 403. FTC RULEMAKING.**

2 The Commission shall initiate a rulemaking within 90
3 days after the date of enactment of this Act for regula-
4 tions to implement the provisions of title I.

5 **SEC. 404. FTC REPORT.**

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

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

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

16 (3) whether legislation is appropriate or nec-
17 essary to regulate the collection, use, and distribu-
18 tion of personally identifiable information collected
19 other than via the Internet;

20 (4) whether and how the government might as-
21 sist industry in developing standard online privacy
22 notices that substantially comply with the require-
23 ments of section 102(a);

24 (5) whether and how the creation of a set of
25 self-regulatory guidelines established by independent
26 safe harbor organizations and approved by the Com-

1 mission would facilitate administration of and com-
2 pliance with title I; and

3 (6) whether additional legislation is necessary
4 or appropriate to regulate the collection, use, and
5 disclosure of personally identifiable information col-
6 lected online before the effective date of title I.

7 (b) FTC NOTICE OF INQUIRY.—The Commission
8 shall initiate a notice of inquiry within 90 days after the
9 date of enactment of this Act to request comment on the
10 matter described in paragraphs (1) through (5) of sub-
11 section (a).

12 **SEC. 405. DEVELOPMENT OF AUTOMATED PRIVACY CON-**
13 **TROLS.**

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

16 (1) by redesignating subsection (d) as sub-
17 section (e); and

18 (2) by inserting after subsection (c) the fol-
19 lowing:

20 “(d) DEVELOPMENT OF INTERNET PRIVACY PRO-
21 GRAM.—The Institute shall encourage and support the de-
22 velopment of one or more computer programs, protocols,
23 or other software, such as the World Wide Web Consor-
24 tium’s P3P program, capable of being installed on com-
25 puters, or computer networks, with Internet access that

1 would reflect the user's preferences for protecting person-
2 ally-identifiable or other sensitive, privacy-related informa-
3 tion, and automatically execute the program, once acti-
4 vated, without requiring user intervention.”.

○