

COMMITTEE AMENDMENT

[STAFF WORKING DRAFT]

May 14, 2002

Purpose: To strengthen the privacy protections afforded by the bill as introduced, and for other purposes.

**IN THE COMMITTEE ON COMMERCE, SCIENCE, AND
TRANSPORTATION—107TH Cong., 2D Sess.**

S. 2201, 107TH Congress, 2D Session

MAY 16, 2002

INTENDED to be proposed by Mr. HOLLINGS

Viz: Strike out all after the enacting clause and insert the following:

1 SECTION 1. SHORT TITLE.

2 This Act may be cited as the “Online Personal Pri-
3 vacy Act”.

4 SEC. 2. TABLE OF CONTENTS.

5 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. Safe harbor self-regulatory programs.

Sec. 204. Private right of action.

Sec. 205. Actions by States.

Sec. 206. Whistleblower protection.

Sec. 207. 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.

Title V—Offline Privacy

Sec. 501. Collection, use, and disclosure of personally identifiable information collected offline.

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-
14 viduals who use the Internet will soon be more
15 gravely threatened.

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

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

3 (6) With the exception of Federal Trade Com-
4 mission enforcement of laws against unfair and de-
5 ceptive practices, the Federal Government thus far
6 has eschewed general Internet privacy laws in favor
7 of industry self-regulation, which has led to several
8 self-policing schemes, some of which are enforceable,
9 and some of which provide insufficient privacy pro-
10 tection to individuals.

11 (7) Many Internet businesses have developed
12 good Internet privacy policies that provide con-
13 sumers notice, choice, access, and security with re-
14 spect to their personal information.

15 (8) Many other Internet businesses, however,
16 have yet to provide these baseline fair information
17 practices, and, absent legislative requirements to the
18 contrary, seem unlikely to do so in the near future.

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

23 (10) States are nonetheless interested in pro-
24 viding greater privacy protection to their citizens as
25 evidenced by recent lawsuits brought against offline

1 and online companies by State attorneys general to
2 protect the privacy of individuals using the Internet.

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

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

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

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

1 (15) Market research demonstrates that as
2 many as one-third of all Internet users give false in-
3 formation about themselves to protect their privacy,
4 due to fears about a lack of privacy protection on
5 the Internet.

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

11 (17) It is important to establish personal pri-
12 vacy rights and industry obligations now so that in-
13 dividuals have confidence that their personal privacy
14 is fully protected on the Internet.

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

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

1 (20) Toward the close of the 20th Century, as
2 individuals' personal information was increasingly
3 collected, profiled, and shared for commercial pur-
4 poses, and as technology advanced to facilitate these
5 practices, the Congress enacted numerous statutes
6 to protect privacy.

7 (21) Those statutes apply to the government,
8 telephones, cable television, e-mail, video tape rent-
9 als, and the Internet (but only with respect to chil-
10 dren).

11 (22) Those statutes all provide significant pri-
12 vacy protections, but neither limit technology nor
13 stifle business.

14 (23) Those statutes ensure that the collection
15 and commercialization of individuals' personal infor-
16 mation is fair, transparent, and subject to law.

17 (24) As in those instances, the Federal govern-
18 ment has a substantial interest in promoting privacy
19 on the Internet.

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

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

1 **TITLE I—ONLINE PRIVACY**
2 **PROTECTION**

3 **SEC. 101. COLLECTION, USE, OR DISCLOSURE OF PERSON-**
4 **ALLY IDENTIFIABLE INFORMATION.**

5 (a) IN GENERAL.—An internet service provider, on-
6 line service provider, or operator of a commercial website
7 on the Internet may not collect personally identifiable in-
8 formation online from a user, or use or disclose personally
9 identifiable information about a user, of that service or
10 website except in accordance with the provisions of this
11 Act.

12 (b) APPLICATION TO CERTAIN THIRD-PARTY OPERA-
13 TORS.—The provisions of this Act applicable to internet
14 service providers, online service providers, and commercial
15 website operators apply to any third party, including an
16 advertising network, that—

17 (1) uses an internet service provider, online
18 service provider, or commercial website operator to
19 collect information about users of that service or
20 website; or

21 (2) makes computer software available to the
22 public, by sale or otherwise, that is capable of—

23 (A) collecting personally identifiable infor-
24 mation about the user, the hardware on which

1 it is used, or the manner in which it is used;
2 and

3 (B) disclosing such information to any per-
4 son other than the user.

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

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

15 (1) the specific types of information that will be
16 collected;

17 (2) the methods of collecting and using the in-
18 formation collected; and

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

23 (b) SENSITIVE PERSONALLY IDENTIFIABLE INFOR-
24 MATION REQUIRES OPT-IN CONSENT.—An internet serv-

1 ice provider, online service provider, or operator of a com-
2 mercial website may not—

3 (1) collect sensitive personally identifiable infor-
4 mation online, or

5 (2) disclose or otherwise use such information
6 collected online, from a user of that service or
7 website,

8 unless the provider or operator obtains that user's consent
9 to the collection and disclosure or use of that information
10 before, or at the time, the information is collected and the
11 user's consent is manifested by an affirmative act in a
12 written or electronic communication.

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

17 (1) collect personally identifiable information
18 not described in subsection (b) online, or

19 (2) disclose or otherwise use such information
20 collected online, from a user of that service or
21 website,

22 unless the provider or operator provides robust notice to
23 the user, in addition to clear and conspicuous notice, and
24 has given the user an opportunity to decline consent for

1 such collection and use by the provider or operator before,
2 or at the time, the information is collected.

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

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

12 (e) PERMANENCE OF CONSENT.—

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

19 (A) shall remain in effect until changed by
20 the user; and

21 (B) shall apply to the collection, disclosure,
22 or other use of that information by any entity
23 that is a commercial successor of, or legal suc-
24 cesssor-in-interest to, that provider or operator,
25 without regard to the legal form in which such

1 succession was accomplished (including any en-
2 tity that collects, discloses, or uses such infor-
3 mation as a result of a proceeding under chap-
4 ter 7 or chapter 11 of title 11, United States
5 Code, with respect to the provider or operator).

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

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

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

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

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

24 (a) NOTICE OF POLICY CHANGE.—Whenever an
25 internet service provider, online service provider, or oper-

1 ator of a commercial website makes a material change in
2 its policy for the collection, use, or disclosure of sensitive
3 or nonsensitive personally identifiable information, it—

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

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

13 (b) NOTICE OF BREACH OF PRIVACY.—

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

18 (A) is disclosed by the provider or operator
19 in violation of any provision of this Act, or

20 (B) the security, confidentiality, or integ-
21 rity of such information is compromised by a
22 hacker or other third party, or by any act or
23 failure to act of the provider or operator and
24 the compromise, act, or failure to act results in

1 a disclosure of personally identifiable informa-
2 tion in violation of any provision of this Act,
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, compromise, act, or failure to
7 act. The notice shall describe the nature of the un-
8 lawful collection, disclosure, use, compromise, act, or
9 failure to act and the steps taken by the provider or
10 operator to remedy it.

11 (2) DELAY OF NOTIFICATION.—

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

21 (i) facilitate the detection and appre-
22 hension of the person responsible for the
23 compromise; 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 such information.

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

17 (i) restore the system's functionality
18 or fix the problem; and

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

1 integrity of the service or website has been
2 restored.

3 **SEC. 104. EXCEPTIONS.**

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

9 (1) to protect the security or integrity of the
10 service or website or to ensure the safety, health, or
11 life of other people or property;

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

15 (3) to provide other products and services or
16 conduct activities integrally related to the trans-
17 action, service, product, or arrangement for which
18 the user provided the information; or

19 (4) to comply with the Fair Credit Reporting
20 Act (15 U.S.C. 1681 et seq.) determined without re-
21 gard to section 603(d)(2) of that Act (15 U.S.C.
22 1681a(d)(2)).

23 (b) PROTECTED DISCLOSURES AND OTHER REGU-
24 LATED ACTIVITIES.—

1 (1) IN GENERAL.—An internet service provider,
2 online service provider, or operator of a commercial
3 website may not be held liable under this Act, any
4 other Federal law, or any State law for any disclo-
5 sure made in good faith and following reasonable
6 procedures in responding to—

7 (A) a request for disclosure of personal in-
8 formation under section 1302(b)(1)(B)(iii) of
9 the Children’s Online Privacy Protection Act of
10 1998 (15 U.S.C. 6501 et seq.) to the parent of
11 a child; or

12 (B) a request for access to, or correction
13 or deletion of, personally identifiable informa-
14 tion under section 105 of this Act.

15 (2) FINANCIAL INSTITUTIONS.—A financial in-
16 stitution (as defined in section 509(3) of the
17 Gramm-Leach-Bliley Act (15 U.S.C. 6809(3)) that
18 is an internet service provider, online service pro-
19 vider, or operator of a commercial website may not
20 be held liable under this Act for any disclosure de-
21 scribed in section 502(e) of that Act (15 U.S.C.
22 6802(e)).

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

1 (1) IN GENERAL.—Notwithstanding any other
2 provision of this Act, an internet service provider,
3 online service provider, operator of a commercial
4 website, or third party that uses such a service or
5 website to collect information about users of that
6 service or website, may disclose personally identifi-
7 able information about a user of that service or
8 website—

9 (A) to a law enforcement, investigatory,
10 national security, or regulatory agency or de-
11 partment of the United States in response to a
12 request or demand made under authority grant-
13 ed to that agency or department by statute,
14 rule, or regulation, or pursuant to a warrant
15 issued under the Federal Rules of Criminal
16 Procedure, an equivalent State warrant, a court
17 order, or a properly executed administrative
18 compulsory process; or

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

23 (i) the user to whom the information
24 relates is given reasonable notice by the
25 person seeking the information of the court

1 proceeding at which the order is requested;

2 and

3 (ii) that user is afforded a reasonable
4 opportunity to appear and contest the
5 issuance of requested order or to narrow
6 its scope.

7 (2) SAFEGUARDS AGAINST FURTHER DISCLO-
8 SURE.—A court that issues an order described in
9 paragraph (1)(B) shall impose appropriate safe-
10 guards on the use of the information to protect
11 against its unauthorized disclosure.

12 (d) EMERGENCY DISCLOSURES.—Notwithstanding
13 any other provision of this Act, an internet service pro-
14 vider, online service provider, operator of a commercial
15 website, or third party that uses such a service or website
16 to collect information about users of that service or
17 website, may disclose personally identifiable information
18 about a user of that service or website to a law enforce-
19 ment officer, hospital, clinic, or other lawful medical orga-
20 nization or a licensed physician or other healthcare profes-
21 sional if—

22 (1) the disclosure is critical to the life, safety,
23 or health of the user or other individuals;

24 (2) it is not feasible under the circumstances to
25 obtain timely consent; and

1 (3) the disclosure is no greater than necessary
2 to accomplish the purpose for which the information
3 is disclosed.

4 (e) DISCLOSURE FOR PROFESSIONAL SERVICES PUR-
5 POSES.—Notwithstanding any other provision of this Act,
6 an internet service provider, online service provider, oper-
7 ator of a commercial website, or third party that uses such
8 a service or website to collect information about users of
9 that service or website, may disclose personally identifiable
10 information about a user of that service or website to a
11 provider of professional services, or any wholly-owned af-
12 filiate thereof, of which the user is a client, patient, or
13 customer if the the provider or affiliate is subject to pro-
14 fessional ethical standards, regulations, rules, or law re-
15 quiring the provider or affiliate not to disclose confidential
16 client information without the consent of the client.

17 **SEC. 105. ACCESS.**

18 (a) IN GENERAL.—An internet service provider, on-
19 line service provider, or operator of a commercial website
20 shall—

21 (1) upon request provide reasonable access to a
22 user to personally identifiable information that the
23 provider or operator has collected and retained from
24 the user online, or that the provider or operator has
25 combined with personally identifiable information

1 collected and retained from the user online after the
2 effective date of this Act;

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

7 (3) make the correction a part of that user's
8 sensitive personally identifiable information or non-
9 sensitive personally identifiable information (which-
10 ever is appropriate), or make the deletion, for all fu-
11 ture disclosure and other use purposes.

12 (b) EXCEPTION.—An internet service provider, online
13 service provider, or operator of a commercial website may
14 decline to make a suggested correction a part of that
15 user's sensitive personally identifiable information or non-
16 sensitive personally identifiable information (whichever is
17 appropriate), or to make a suggested deletion if the pro-
18 vider or operator—

19 (1) reasonably believes that the suggested cor-
20 rection or deletion is inaccurate or otherwise inap-
21 propriate;

22 (2) notifies the user in writing, or in digital or
23 other electronic form, of the reasons the provider or
24 operator believes the suggested correction or deletion
25 is inaccurate or otherwise inappropriate; and

1 (3) provides a reasonable opportunity for the
2 user to refute the reasons given by the provider or
3 operator for declining to make the suggested correc-
4 tion or deletion.

5 (c) REASONABLENESS TEST.—The reasonableness of
6 the access or opportunity provided under subsection (a)
7 or (b) by an internet service provider, online service pro-
8 vider, or operator of a commercial website shall be deter-
9 mined by taking into account such factors as the sensi-
10 tivity of the information requested and the burden or ex-
11 pense on the provider or operator of complying with the
12 request, correction, or deletion.

13 (d) REASONABLE ACCESS FEE.—

14 (1) IN GENERAL.—An internet service provider,
15 online service provider, or operator of a commercial
16 website may impose a reasonable charge for access
17 under subsection (a).

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

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

1 (B) is a recipient of public welfare assist-
2 ance; or

3 (C) has reason to believe that the incorrect
4 information is due to fraud.

5 **SEC. 106. SECURITY.**

6 An internet service provider, online service provider,
7 or operator of a commercial website shall establish and
8 maintain reasonable procedures necessary to protect the
9 security, confidentiality, and integrity of personally identi-
10 fiable information maintained by that provider or oper-
11 ator.

12 **TITLE II—ENFORCEMENT**

13 **SEC. 201. ENFORCEMENT BY FEDERAL TRADE COMMIS-**
14 **SION.**

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

18 **SEC. 202. VIOLATION IS UNFAIR OR DECEPTIVE ACT OR**
19 **PRACTICE.**

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

1 (b) ENFORCEMENT BY CERTAIN OTHER AGEN-
2 CIES.—Compliance with title I of this Act shall be
3 enforced—

4 (1) under section 8 of the Federal Deposit In-
5 surance Act (12 U.S.C. 1818), in the case of—

6 (A) national banks, and Federal branches
7 and Federal agencies of foreign banks, and any
8 subsidiaries of such entities (except brokers,
9 dealers, persons providing insurance, invest-
10 ment companies, and investment advisers), by
11 the Office of the Comptroller of the Currency;

12 (B) member banks of the Federal Reserve
13 System (other than national banks), branches
14 and agencies of foreign banks (other than Fed-
15 eral branches, Federal agencies, and insured
16 State branches of foreign banks), commercial
17 lending companies owned or controlled by for-
18 eign banks, organizations operating under sec-
19 tion 25 or 25A of the Federal Reserve Act (12
20 U.S.C. 601 and 611), and bank holding compa-
21 nies and their nonbank subsidiaries or affiliates
22 (except brokers, dealers, persons providing in-
23 surance, investment companies, and investment
24 advisers), by the Board;

1 (C) banks insured by the Federal Deposit
2 Insurance Corporation (other than members of
3 the Federal Reserve System) insured State
4 branches of foreign banks, and any subsidiaries
5 of such entities (except brokers, dealers, per-
6 sons providing insurance, investment compa-
7 nies, and investment advisers), by the Board of
8 Directors of the Federal Deposit Insurance Cor-
9 poration; and

10 (D) savings associations the deposits of
11 which are insured by the Federal Deposit In-
12 surance Corporation, and any subsidiaries of
13 such savings associations (except brokers, deal-
14 ers, persons providing insurance, investment
15 companies, and investment advisers), by the Di-
16 rector of the Office of Thrift Supervision;

17 (2) under the Federal Credit Union Act (12
18 U.S.C. 1751 et seq.) by the Board of the National
19 Credit Union Administration with respect to any
20 Federally insured credit union, and any subsidiaries
21 of such a credit union;

22 (3) under the Securities Exchange Act of 1934
23 (15 U.S.C. 78a et seq.) by the Securities and Ex-
24 change Commission with respect to any broker or
25 dealer;

1 (4) under the Investment Company Act of 1940
2 (15 U.S.C. 80a-1 et seq.) by the Securities and Ex-
3 change Commission with respect to investment com-
4 panies;

5 (5) under the Investment Advisers Act of 1940
6 (15 U.S.C. 80b-1 et seq.) by the Securities and Ex-
7 change Commission with respect to investment ad-
8 visers registered under that Act;

9 (6) under State insurance law in the case of
10 any person engaged in providing insurance, by the
11 applicable State insurance authority of the State in
12 which the person is domiciled, subject to section 104
13 of the Gramm-Bliley-Leach Act (15 U.S.C. 6701);

14 (7) under part A of subtitle VII of title 49,
15 United States Code, by the Secretary of Transpor-
16 tation with respect to any air carrier or foreign air
17 carrier subject to that part;

18 (8) under the Packers and Stockyards Act,
19 1921 (7 U.S.C. 181 et seq.) (except as provided in
20 section 406 of that Act (7 U.S.C. 226, 227)), by the
21 Secretary of Agriculture with respect to any activi-
22 ties subject to that Act;

23 (9) under the Farm Credit Act of 1971 (12
24 U.S.C. 2001 et seq.) by the Farm Credit Adminis-
25 tration with respect to any Federal land bank, Fed-

1 eral land bank association, Federal intermediate
2 credit bank, or production credit association; and

3 (10) under title XI of the Social Security Act
4 (42 U.S.C. 1301 et seq.) by the Secretary of Health
5 and Human Services with respect to persons regu-
6 lated under that title.

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

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

1 Trade Commission Act in the same manner, by the same
2 means, and with the same jurisdiction, power, and duties
3 as though all applicable terms and provisions of the Fed-
4 eral Trade Commission Act were incorporated into and
5 made a part of that subtitle.

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

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

16 (A) paid to the Commission;

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

19 (C) distributed in accordance with para-
20 graph (2).

21 (2) DISTRIBUTION TO USERS.—Under proce-
22 dures to be established by the Commission, the Com-
23 mission shall hold any amount received as a civil
24 penalty for violation of title I for a period of not less

1 than 180 days for distribution under those proce-
2 dures to users—

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

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

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

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

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

19 (4) REMAINDER.—If the amount of any such
20 penalty held by the Commission exceeds the sum of
21 the amounts distributed under paragraph (2) attrib-
22 utable to that penalty, the excess shall be covered
23 into the Treasury of the United States as miscella-
24 neous receipts no later than 12 months after it was
25 paid to the Commission.

1 (f) EFFECT ON OTHER LAWS.—

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

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

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

16 “(i) With respect to the provision by a cable operator
17 of Internet service or online service and the operation by
18 a cable operator of a commercial website, as such terms
19 are defined in or under the Online Personal Privacy Act,
20 the provisions of that Act shall apply in lieu of this sec-
21 tion.”.

22 **SEC. 203. SAFE HARBOR SELF-REGULATORY PROGRAMS.**

23 (a) IN GENERAL.—An internet service provider, on-
24 line service provider, or operator of a commercial website

1 shall be presumed to be in compliance with the require-
2 ments of this title if the provider or operator—

3 (1) is a participant in a self-regulatory program
4 approved by the Commission under subsection (b)
5 and has agreed in writing to meet the requirements
6 for participation established by the self-regulatory
7 program; and

8 (2) is deemed by the self-regulatory program to
9 be in full compliance with the requirements of that
10 self-regulatory program.

11 (b) APPROVAL OF SELF-REGULATORY PROGRAMS.—
12 The Commission may approve a self-regulatory program
13 under subsection (a) only if the Commission finds the fol-
14 lowing:

15 (1) PARTICIPATION REQUIREMENTS.—The self-
16 regulatory program will require participants, at a
17 minimum, to provide privacy protection to users of
18 the internet service, online service, or commercial
19 website that is substantially equivalent to or greater
20 than the protection afforded to users by title I.

21 (2) ELIGIBILITY AND VERIFICATION.—The self-
22 regulatory program—

23 (A) will require, prior to determining eligi-
24 bility to participate in the self-regulatory pro-

1 gram, and on a periodic basis thereafter no less
2 frequent than annually—

3 (i) a review by the self-regulatory pro-
4 gram or a certified independent verification
5 organization of the prospective partici-
6 pant's privacy statement and privacy pol-
7 icy; and

8 (ii) a determination by the self-regu-
9 latory program or a certified independent
10 verification organization that the privacy
11 statement and privacy policy comply with
12 the self-regulatory program's requirements;

13 (B) will obtain, prior to determining eligi-
14 bility to participate in the self-regulatory pro-
15 gram, and on a periodic basis thereafter no less
16 frequently than annually, a written certification
17 from a senior corporate officer or other respon-
18 sible executive of the participant that—

19 (i) the participant has procedures and
20 practices in place that are designed to ful-
21 fill the representations in the participant's
22 privacy policy and satisfy, at a minimum
23 the requirements of the self-regulatory pro-
24 gram; and

1 (ii) the participant is in compliance
2 with the privacy policy and the require-
3 ments of the self-regulatory program;

4 (C) will require each participant to obtain
5 written verification of each written certification
6 required by subparagraph (B) from a certified
7 independent verification organization or provide
8 sufficient information to the self-regulatory pro-
9 gram to enable the program reasonably to con-
10 clude that the certification is materially accu-
11 rate; and

12 (D) has a program for verification of con-
13 tinued eligibility of program participants under
14 which program resources are effectively utilized
15 to ensure compliance with, and discover viola-
16 tions of, the self-regulatory program's require-
17 ments, including random audits of participants.

18 (4) TRANSPARENCY.—The self-regulatory pro-
19 gram will make available to the public via the Inter-
20 net the results of audits and violations of the pro-
21 gram's requirements, excluding information that
22 would reveal the identity of any complainant whose
23 privacy was violated.

24 (5) COOPERATION WITH COMMISSION.—The
25 self-regulatory program, and any independent

1 verification organization used by participants in that
2 program, will report to the Commission any viola-
3 tions of its requirements by participants and any de-
4 terminations that a participant has failed to comply
5 with the self-regulatory program requirements after
6 being afforded a reasonable opportunity to do so.

7 (6) INDEPENDENCE.—The self-regulatory pro-
8 gram has established requirements that assure that
9 program eligibility and compliance determinations
10 concerning a participant are made exclusively by
11 persons who are independent of the participant.

12 (c) COMMISSION TO MONITOR COMPLIANCE.—

13 (1) PUBLICATION OF REPORTED FAILURES TO
14 COMPLY.—The Commission shall publish a list of all
15 violations reported to it by self-regulatory programs
16 and independent verification organizations.

17 (2) BIENNIAL REVIEW.—The Commission shall
18 re-evaluate its approval of each self-regulatory pro-
19 gram under subsection (b) at least once every 2
20 years.

21 (d) CERTIFICATION OF INDEPENDENT VERIFICATION
22 ORGANIZATIONS.—

23 (1) IN GENERAL.—The Commission may certify
24 an entity as an independent verification organization
25 for purposes of this section. In carrying out this

1 subsection, the Commission shall consider both the
2 technical expertise and the experience of a prospec-
3 tive independent verification organization in pro-
4 viding assurance services.

5 (2) ELIGIBLE ENTITIES.—An independent
6 verification organization may be—

7 (A) a self-regulatory program, but only
8 with respect to an internet service provider, on-
9 line service provider, or commercial website op-
10 erator that is not a participant in that program;
11 or

12 (B) any other entity that provides assur-
13 ance services and that demonstrates to the sat-
14 isfaction of the Commission that it has the abil-
15 ity and knowledge required to examine and
16 evaluate the business practices of a participant
17 or prospective participant.

18 (e) APPLICATION PROCESS.—

19 (1) APPLICATION.—The Commission shall es-
20 tablish an application process for the approval of a
21 self-regulatory program under subsection (b). The
22 application shall be submitted at such time, in such
23 manner, and contain such information as the Com-
24 mission may require. Upon receipt of an application,
25 the Commission shall provide notice of the applica-

1 tion and an opportunity for comment on the applica-
2 tion to the public. The Commission shall make a de-
3 cision on an application within 120 days after re-
4 ceipt of the application.

5 (2) APPEAL.—A self-regulatory program that is
6 aggrieved by final action of the Commission or a
7 failure by the Commission to take action on a timely
8 basis as required by paragraph (1) may file an ac-
9 tion in a district court under section 706 of title 5,
10 United States Code, to obtain review of the decision
11 without regard to the amount in controversy.

12 (f) UNAUTHORIZED CLAIM OF PARTICIPATION.—An
13 internet service provider, online service provider, or oper-
14 ator of a commercial website that willfully and falsely rep-
15 resents to the public by a statement, display of an emblem,
16 or otherwise that it is a participant in an approved self-
17 regulatory program under this section shall be liable for
18 a civil penalty of up to \$50,000 for each such false rep-
19 resentation. The civil penalty may be recovered in an ac-
20 tion brought by the Commission or a State attorney gen-
21 eral in any court of competent jurisdiction.

22 (g) QUALIFIED PRIVILEGE.—A self-regulatory pro-
23 gram is not liable to any person as a result of a publication
24 under subsection (b)(4) unless it is found to have acted
25 with malice or recklessness.

1 **SEC. 204. PRIVATE RIGHTS OF ACTION BY USERS.**

2 (a) FRAUDULENT NOTICE; WRONGFUL DISCLO-
3 SURE.—A person to whom fraudulent notice with respect
4 to sensitive personally identifiable information was given
5 under this Act or whose sensitive personally identifiable
6 information has been disclosed in violation of title I, may,
7 if otherwise permitted by the laws or rules of court of a
8 State, bring in an appropriate court of that State—

9 (1) an action based on the violation to enjoin
10 the violation;

11 (2) an action to recover the amount of any ac-
12 tual monetary loss from the violation or, to receive
13 up to \$500 in damages for each such violation,
14 whichever is greater; or

15 (3) both such actions.

16 (b) OTHER VIOLATIONS.—A person harmed by any
17 violation of title I not described in subsection (a) but re-
18 lated to sensitive personally identifiable information may,
19 if otherwise permitted by the laws or rules of court of a
20 State, bring in an appropriate court of that State—

21 (1) an action based on the violation to enjoin
22 the violation;

23 (2) an action to recover the amount of any ac-
24 tual monetary loss from the violation; or

25 (3) both such actions.

1 (c) AFFIRMATIVE DEFENSE.—It shall be an affirma-
2 tive defense in any action brought under this section that
3 the defendant—

4 (1) has established and implemented with due
5 care reasonable practices and procedures to ensure
6 compliance with the requirements of title I; or

7 (2) is a participant in, and is deemed by a self-
8 regulatory organization or a certified independent
9 verification organization to be in full compliance
10 with the requirements of, a self-regulatory program
11 approved by the Commission under section 203.

12 (d) WILLFUL OR KNOWING VIOLATIONS.—If the
13 court finds that the defendant willfully or knowingly vio-
14 lated title I, the court may, in its discretion, increase the
15 amount of the award to an amount equal to not more than
16 3 times the amount available under this section.

17 **SEC. 205. ACTIONS BY STATES.**

18 (a) IN GENERAL.—

19 (1) CIVIL ACTIONS.—In any case in which the
20 attorney general of a State has reason to believe
21 that an interest of the residents of that State has
22 been or is threatened or adversely affected by the
23 engagement of any person in a practice that violates
24 title I, the State, as *parens patriae*, may bring a civil
25 action on behalf of the residents of the State in a

1 district court of the United States of appropriate
2 jurisdiction—

3 (A) to enjoin that practice;

4 (B) to enforce compliance with the rule;

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

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

10 (2) NOTICE.—

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

15 (i) written notice of that action; and

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

18 (B) EXEMPTION.—

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

1 (ii) NOTIFICATION.—In an action de-
2 scribed in clause (i), the attorney general
3 of a State shall provide notice and a copy
4 of the complaint to the Commission at the
5 same time as the attorney general files the
6 action.

7 (b) INTERVENTION.—

8 (1) IN GENERAL.—On receiving notice under
9 subsection (a)(2), the Commission shall have the
10 right to intervene in the action that is the subject
11 of the notice.

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

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

17 (B) to file a petition for appeal.

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

23 (1) conduct investigations;

24 (2) administer oaths or affirmations; or

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

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

9 (e) VENUE; SERVICE OF PROCESS.—

10 (1) VENUE.—Any action brought under sub-
11 section (a) may be brought in the district court of
12 the United States that meets applicable require-
13 ments relating to venue under section 1391 of title
14 28, United States Code.

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

18 (A) is an inhabitant; or

19 (B) may be found.

20 **SEC. 206. WHISTLEBLOWER PROTECTION.**

21 (a) IN GENERAL.—No internet service provider, on-
22 line service provider, or commercial website operator may
23 discharge or otherwise discriminate against any employee
24 with respect to compensation, terms, conditions, or privi-
25 leges of employment because the employee (or any person

1 acting pursuant to the request of the employee) provided
2 information to any Federal or State agency or to the At-
3 torney General of the United States or of any State re-
4 garding a violation of any provision of title I.

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

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

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

20 (2) to pay compensatory damages; or

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

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

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

3 (2) knowingly or recklessly provides substan-
4 tially false information to such an agency or the At-
5 torney General.

6 (e) BURDENS OF PROOF.—The legal burdens of proof
7 that prevail under subchapter III of chapter 12 of title
8 5, United States Code (5 U.S.C. 1221 et seq.) shall govern
9 adjudication of protected activities under this section.

10 **SEC. 207. NO EFFECT ON OTHER REMEDIES.**

11 The remedies provided by sections 204 and 205 are
12 in addition to any other remedy available under any provi-
13 sion of law.

14 **TITLE III—APPLICATION TO**
15 **CONGRESS AND FEDERAL**
16 **AGENCIES**

17 **SEC. 301. SENATE.**

18 The Sergeant at Arms of the United States Senate
19 shall develop regulations setting forth an information se-
20 curity and electronic privacy policy governing use of the
21 Internet by officers and employees of the Senate that
22 meets the requirements of title I.

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

24 (a) IN GENERAL.—Except as provided in subsection
25 (b), this Act applies to each Federal agency that is an

1 internet service provider or an online service provider, or
2 that operates a website, to the extent provided by section
3 2674 of title 28, United States Code.

4 (b) EXCEPTIONS.—This Act does not apply to any
5 Federal agency to the extent that the application of this
6 Act would compromise law enforcement activities or the
7 administration of any investigative, security, or safety op-
8 eration conducted in accordance with Federal law.

9 **TITLE IV—MISCELLANEOUS**

10 **SEC. 401. DEFINITIONS.**

11 In this Act:

12 (1) COLLECT.—

13 (A) IN GENERAL.—The term “collect”
14 means the online gathering of personally identi-
15 fiable information from a user of an Internet
16 service, online service, or commercial website by
17 or on behalf of the provider or operator of that
18 service or website by any means, direct or indi-
19 rect, active or passive, including—

20 (i) an online request for such informa-
21 tion by the provider or operator, regardless
22 of how the information is transmitted to
23 the provider or operator;

24 (ii) the use of a chat room, a message
25 board, e-mail, instant messaging, or any

1 other online service to gather the informa-
2 tion; or

3 (iii) tracking or use of any identifying
4 code linked to a user of such a service or
5 website, including the use of cookies or
6 other tracking technology.

7 (B) TEMPORARY COLLECTION OR STORAGE
8 EXCEPTION.—Notwithstanding subparagraph
9 (A)(ii), the term “collect” does not include the
10 temporary collection or storage of information
11 by a chat room, message board, e-mail server,
12 instant messaging service, or other online serv-
13 ice for the sole purpose of operating that chat
14 room, message board, e-mail server, instant
15 messaging service, or other online service.

16 (2) COMMISSION.—The term “Commission”
17 means the Federal Trade Commission.

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

24 (4) DISCLOSE.—The term “disclose” means the
25 release of personally identifiable information about a

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

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

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

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

1 (8) INTERNET SERVICE PROVIDER; ONLINE
2 SERVICE PROVIDER; WEBSITE.—The Commission
3 shall by rule define the terms “internet service pro-
4 vider”, “online service provider”, and “website”, and
5 shall revise or amend such rule to take into account
6 changes in technology, practice, or procedure with
7 respect to the collection of personal information over
8 the Internet.

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

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

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

1 sale through that website or online service, in-
2 volving commerce—

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

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

8 (I) another such territory; or

9 (II) any State or foreign nation;

10 or

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

13 but

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

18 (11) PERSONALLY IDENTIFIABLE INFORMA-
19 TION.—

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

1 (i) a first and last name, whether
2 given at birth or adoption, assumed, or le-
3 gally changed;

4 (ii) a home or other physical address
5 including street name and name of a city
6 or town;

7 (iii) an e-mail address;

8 (iv) a telephone number;

9 (v) a birth certificate number;

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

15 (vii) information that an Internet
16 service provider, online service provider, or
17 operator of a commercial website combines
18 with an identifier described in clauses (i)
19 through (vi) of this subparagraph.

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

1 (12) RELEASE.—The term “release of person-
2 ally identifiable information” means the direct or in-
3 direct, sharing, selling, renting, or other provision of
4 personally identifiable information of a user of an
5 internet service, online service, or commercial
6 website to any other person other than the user.

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

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

16 (A) the amount of income earned or losses
17 suffered by an individual;

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

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

1 (D) an individual's insurance policy infor-
2 mation, including the existence, premium, face
3 amount, or coverage limits of an insurance pol-
4 icy held by or for the benefit of an individual;
5 or

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

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

12 (A) individually identifiable health infor-
13 mation (as defined in section 164.501 of title
14 45, Code of Federal Regulations);

15 (B) race or ethnicity;

16 (C) political party affiliation;

17 (D) religious beliefs;

18 (E) sexual orientation;

19 (F) a Social Security number; or

20 (G) sensitive financial information.

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

22 Title I of this Act takes effect on the day after the
23 date on which the Commission publishes a final rule under
24 section 403.

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

2 The Commission shall—

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

6 (2) complete that rulemaking within 270 days
7 after initiating it.

8 **SEC. 404. FTC REPORT.**

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

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

16 (2) whether technology that protects privacy is
17 being utilized in the marketplace in such a manner
18 as to facilitate administration of and compliance
19 with title I;

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

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

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

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

10 **SEC. 405. DEVELOPMENT OF AUTOMATED PRIVACY CON-**
11 **TROLS.**

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

14 (1) by redesignating subsection (d) as sub-
15 section (e); and

16 (2) by inserting after subsection (c) the fol-
17 lowing:

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

1 tion, and automatically execute the program, once acti-
2 vated, without requiring user intervention.”.

3 **TITLE V—OFFLINE PRIVACY]**

4 **SEC. 501. COLLECTION, USE, AND DISCLOSURE OF PERSON-**
5 **ALLY IDENTIFIABLE INFORMATION COL-**
6 **LECTED OFFLINE.**

7 (a) IN GENERAL.—Not later than the date that is
8 6 months after the date of the enactment of this Act, the
9 Chairman of the Federal Trade Commission shall submit
10 to the Committee on Commerce, Science, and Transpor-
11 tation of the United States Senate, and the Committee
12 on Energy and Commerce of the United States House of
13 Representatives, detailed recommendations and proposed
14 regulations on standards with respect to entities that en-
15 gage in the collection of personally identifiable informa-
16 tion, or employ methods involving, or other actions involv-
17 ing, the collection of personally identifiable information,
18 that are not covered in this Act, at a level of protection
19 similar to that provided under this Act for similar types
20 of information.

21 (b) SUBJECTS FOR RECOMMENDATIONS.—The rec-
22 ommendations and proposed regulations under subsection
23 (a) shall address at least the following:

24 (1) How the fair information practices of no-
25 tice, choice, access, security, and enforcement should

1 apply to the uses and disclosures of such informa-
2 tion in a manner consistent with the level of protec-
3 tion provided by this Act.

4 (2) The fines that should be established for vio-
5 lating requirements promulgated under the regula-
6 tions.

7 (c) REGULATIONS.—

8 (1) CONTINGENT ON LEGISLATION.—If an Act
9 of Congress that—

10 (A) establishes standards with respect to
11 entities that engage in the collection of person-
12 ally identifiable information, or employ methods
13 or other actions involving the collection of per-
14 sonally identifiable information that are not
15 covered in this Act, and

16 (B) refers to this paragraph,
17 does not become law within 18 months after the
18 date of enactment of this Act, then the Commission
19 shall promulgate final regulations (addressing at
20 least the subjects described in subsection (b)) con-
21 taining such standards not later than the date that
22 is 19 months after the date of enactment of this Act.

23 (2) PREEMPTION.—A regulation promulgated
24 under paragraph (1) shall supersede State law only

1 to the extent that this Act supersedes State law
2 under section 4 of this Act.

○