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

IN THE SENATE OF THE UNITED STATES

APRIL 18, 2002

Mr. Hollings (for himself, Mr. Stevens, Mr. Burns, Mr. Inouye, Mr. Rockefeller, Mr. Kerry, Mr. Breaux, Mrs. Carnahan, Mr. Cleland, and Mr. Nelson of Florida) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation.

A BILL

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

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

SECTION 1. SHORT TITLE.

This Act may be cited as the “Online Personal Privacy Act”.

SEC. 2. TABLE OF CONTENTS.

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
The Congress finds the following:

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

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

(3) Absent the recognition of these rights and the establishment of consequent industry responsibilities to safeguard those rights, the privacy of indi-
individuals who use the Internet will soon be more
gravely threatened.

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

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

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

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

(8) States are nonetheless interested in pro-
viding greater privacy protection to their citizens as
evidenced by recent lawsuits brought against offline
and online companies by State attorneys general to
protect the privacy of individuals using the Internet.
(9) The ease of gathering and compiling personal information on the Internet, both overtly and surreptitiously, is becoming increasingly efficient and effortless due to advances in digital communications technology which have provided information gatherers the ability to compile seamlessly highly detailed personal histories of Internet users.

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

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

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

(13) Market research demonstrates that as many as one-third of all Internet users give false information about themselves to protect their privacy,
due to fears about a lack of privacy protection on
the Internet.

(14) Notwithstanding these concerns, the Inter-
net is becoming a major part of the personal and
commercial lives of millions of Americans, providing
increased access to information, as well as commun-
ications and commercial opportunities.

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

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

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

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

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

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

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

SEC. 4. PREEMPTION OF STATE LAW OR REGULATIONS.

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

TITLE I—ONLINE PRIVACY
PROTECTION

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

(a) In General.—An internet service provider, on-
line service provider, or operator of a commercial website
on the Internet may not collect personally identifiable in-
formation from a user, or use or disclose personally identi-
liable information about a user, of that service or website except in accordance with the provisions of this Act.

(b) Application to Certain Third-Party Operators.—The provisions of this Act applicable to internet service providers, online service providers, and commercial website operators apply to any third party, including an advertising network, that uses an internet service provider, online service provider, or commercial website operator to collect information about users of that service or website.

SEC. 102. NOTICE AND CONSENT REQUIREMENTS.

(a) Notice.—Except as provided in section 104, an internet service provider, online service provider, or operator of a commercial website may not collect personally identifiable information from a user of that service or website online unless that provider or operator provides clear and conspicuous notice to the user in the manner required by this section for the kind of personally identifiable information to be collected. The notice shall disclose—

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

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

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

(b) Sensitive Personally Identifiable Information Requires Opt-in Consent.—An internet service provider, online service provider, or operator of a commercial website may not—

(1) collect sensitive personally identifiable information online, or

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

unless the provider or operator obtains that user’s affirmative consent to the collection and disclosure or use of that information before, or at the time, the information is collected.

e) Nonsensitive Personally Identifiable Information Requires Robust Notice and Opt-out Consent.—An internet service provider, online service provider, or operator of a commercial website may not—

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

(2) disclose or otherwise use such information collected online, from a user of that service or website,
unless the provider or operator provides robust notice to
the user, in addition to clear and conspicuous notice, and
has given the user an opportunity to decline consent for
such collection and use by the provider or operator before,
or at the time, the information is collected.

(d) Initial Notice Only for Robust Notice.—

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

(e) Permanence of Consent.—

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

(A) shall remain in effect until changed by
the user; and
(B) shall apply to the collection, disclosure, or other use of that information by any entity that is a commercial successor of, or legal successor-in-interest to, that provider or operator, without regard to the legal form in which such succession was accomplished (including any entity that collects, discloses, or uses such information as a result of a proceeding under chapter 7 or chapter 11 of title 11, United States Code, with respect to the provider or operator).

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

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

(B) the methods of collecting and using the information employed by the successor entity are materially different from the methods employed by the predecessor entity; or
(C) the disclosure practices of the successor entity are materially different from the practices of the predecessor entity.

SEC. 103. POLICY CHANGES; BREACH OF PRIVACY.

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

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

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

(b) NOTICE OF BREACH OF PRIVACY.—

(1) IN GENERAL.—If the sensitive or nonsensitive personally identifiable information of a user of an internet service provider, online service provider, or operator of a commercial website—
(A) is collected, disclosed, or otherwise
used by the provider or operator in violation of
any provision of this Act, or

(B) the security, confidentiality, or integ-
riety of such information is compromised by a
hacker or other third party, or by any act or
failure to act of the provider or operator,
then the provider or operator shall notify all users
whose sensitive or nonsensitive personally identifi-
able information was affected by the unlawful collec-
tion, disclosure, use, or compromise. The notice shall
describe the nature of the unlawful collection, disclo-
sure, use, or compromise and the steps taken by the
provider or operator to remedy it.

(2) DELAY OF NOTIFICATION.—

(A) ACTION TAKEN BY INDIVIDUALS.—If
the compromise of the security, confidentiality,
or integrity of the information is caused by a
hacker or other external interference with the
service or website, or by an employee of the
service or website, the provider or operator may
postpone issuing the notice required by para-
graph (1) for a reasonable period of time in
order to—
(i) facilitate the detection and apprehension of the person responsible for the compromise; and

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

(B) SYSTEM FAILURES AND OTHER FUNCTIONAL CAUSES.—If the unlawful collection, disclosure, use, or compromise of the security, confidentiality, and integrity of the information is the result of a system failure, a problem with the operating system, software, or program used by the internet service provider, online service provider, or operator of the commercial website, or other non-external interference with the service or website, the provider or operator may postpone issuing the notice required by paragraph (1) for a reasonable period of time in order to—

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

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

SEC. 104. EXCEPTIONS.

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

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

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

(3) to provide other products and services integrally related to the transaction, service, product, or arrangement for which the user provided the information.

(b) PROTECTED DISCLOSURES.—An internet service provider, online service provider, or operator of a commercial website may not be held liable under this Act, any
other Federal law, or any State law for any disclosure
made in good faith and following reasonable procedures
in responding to—

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

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

c Disclosure to Law Enforcement Agency or
under Court Order.—

(1) In general.—Notwithstanding any other
provision of this Act, an internet service provider,
online service provider, operator of a commercial
website, or third party that uses such a service or
website to collect information about users of that
service or website may disclose personally identifi-
able information about a user of that service or
website—

(A) to a law enforcement, investigatory,
national security, or regulatory agency or de-
partment of the United States in response to a
request or demand made under authority grant-
ed to that agency or department, including a
warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a court order, or a properly executed administrative compulsory process; and

(B) in response to a court order in a civil proceeding granted upon a showing of compelling need for the information that cannot be accommodated by any other means if—

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

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

(2) Safeguards Against Further Disclosure.—A court that issues an order described in paragraph (1) shall impose appropriate safeguards on the use of the information to protect against its unauthorized disclosure.
SEC. 105. ACCESS.

(a) IN GENERAL.—An internet service provider, online service provider, or operator of a commercial website shall—

(1) upon request provide reasonable access to a user to personally identifiable information that the provider or operator has collected from the user online, or that the provider or operator has combined with personally identifiable information collected from the user online after the effective date of this Act;

(2) provide a reasonable opportunity for a user to suggest a correction or deletion of any such information maintained by that provider or operator to which the user was granted access; and

(3) make the correction a part of that user’s sensitive personally identifiable information or non-sensitive personally identifiable information (whichever is appropriate), or make the deletion, for all future disclosure and other use purposes.

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

(1) reasonably believes that the suggested correction or deletion is inaccurate or otherwise inappropriate;

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

(3) provides a reasonable opportunity for the user to refute the reasons given by the provider or operator for declining to make the suggested correction or deletion.

(e) Reasonableness Test.—The reasonableness of the access or opportunity provided under subsection (a) or (b) by an internet service provider, online service provider, or operator of a commercial website shall be determined by taking into account such factors as the sensitivity of the information requested and the burden or expense on the provider or operator of complying with the request, correction, or deletion.

(d) Reasonable Access Fee.—

(1) In general.—An internet service provider, online service provider, or operator of a commercial
website may impose a reasonable charge for access under subsection (a).

(2) AMOUNT.—The amount of the fee shall not exceed $3, except that upon request of a user, a provider or operator shall provide such access without charge to that user if the user certifies in writing that the user—

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

(B) is a recipient of public welfare assistance; or

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

SEC. 106. SECURITY.

An internet service provider, online service provider, or operator of a commercial website shall establish and maintain reasonable procedures necessary to protect the security, confidentiality, and integrity of personally identifiable information maintained by that provider or operator.
TITLE II—ENFORCEMENT

SEC. 201. ENFORCEMENT BY FEDERAL TRADE COMMISSION.

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

SEC. 202. VIOLATION IS UNFAIR OR DECEPTIVE ACT OR PRACTICE.

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

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

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

(A) national banks, and Federal branches and Federal agencies of foreign banks, by the

Office of the Comptroller of the Currency;

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

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

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

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

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

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

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

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

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

(e) Disposition of Civil Penalties Obtained by
FTC Enforcement Action Involving Nonsensitive
Personally Identifiable Information.—

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

(A) paid to the Commission;

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

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

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

(A) whose nonsensitive personally identifiable information was the subject of the violation; and

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

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

(i) shall not exceed $200; and

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

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

(f) **Effect on Other Laws.**—

(1) **Preservation of Commission Authority.**—Nothing contained in this subtitle shall be construed to limit the authority of the Commission under any other provision of law.

(2) **Relation to Title II of Communications Act.**—Nothing in title I requires an operator of a website or online service to take any action that is inconsistent with the requirements of section 222 of the Communications Act of 1934 (47 U.S.C. 222).

(3) **Relation to Title VI of Communications Act.**—Section 631 of the Communications Act of 1934 (47 U.S.C. 551) is amended by adding at the end the following:

“(i) To the extent that the application of any provision of this title to a cable operator as an internet service provider, online service provider, or operator of a commercial website (as those terms are defined in section 401 of the Online Personal Privacy Act) with respect to the provision of Internet service or online service, or the operation of a commercial website, conflicts with the application of any provision of that Act to such provision or operation,
the Act shall be applied in lieu of the conflicting provision of this title.”

SEC. 203. ACTIONS BY USERS.

(a) Private Right of Action for Sensitive Personally Identifiable Information.—If an internet service provider, online service provider, or commercial website operator collects, discloses, or uses the sensitive personally identifiable information of any person or fails to provide reasonable access to or reasonable security for such sensitive personally identifiable information in violation of any provision of title I then that person may bring an action in a district court of the United States of appropriate jurisdiction—

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

(2) upon a showing of actual harm to that person caused by the violation, to recover the greater of—

(A) the actual monetary loss from the violation; or

(B) $5,000.

(b) Repeated Violations.—If the court finds, in an action brought under subsection (a) to recover damages, that the defendant repeatedly and knowingly violated title I, the court may, in its discretion, increase the
amount of the award available under subsection (a)(2)(B) to an amount not in excess of $100,000.

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

SEC. 204. ACTIONS BY STATES.

(a) IN GENERAL.—

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

(A) to enjoin that practice;

(B) to enforce compliance with the rule;
(C) to obtain damage, restitution, or other
compensation on behalf of residents of the
State; or

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

(2) NOTICE.—

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

(i) written notice of that action; and

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

(B) EXEMPTION.—

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

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

(b) INTERVENTION.—

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

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

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

(B) to file a petition for appeal.

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

(1) conduct investigations;

(2) administer oaths or affirmations; or

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

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

(e) Venue; Service of Process.—

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

(2) Service of Process.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

SEC. 205. WHISTLEBLOWER PROTECTION.

(a) In General.—No internet service provider, online service provider, or commercial website operator may discharge or otherwise discriminate against any employee with respect to compensation, terms, conditions, or privileges of employment because the employee (or any person acting pursuant to the request of the employee) provided information to any Federal or State agency or to the Attorney General of the United States or of any State regarding a violation of any provision of title I.
(b) ENFORCEMENT.—Any employee or former employee who believes he has been discharged or discriminated against in violation of subsection (a) may file a civil action in the appropriate United States district court before the close of the 2-year period beginning on the date of such discharge or discrimination. The complainant shall also file a copy of the complaint initiating such action with the appropriate Federal agency.

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

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

(2) to pay compensatory damages; or

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

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

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

(2) knowingly or recklessly provides substantially false information to such an agency or the Attorney General.
(c) BURDENS OF PROOF.—The legal burdens of proof that prevail under subchapter III of chapter 12 of title 5, United States Code (5 U.S.C. 1221 et seq.) shall govern adjudication of protected activities under this section.

SEC. 206. NO EFFECT ON OTHER REMEDIES.

The remedies provided by sections 203 and 204 are in addition to any other remedy available under any provision of law.

TITLE III—APPLICATION TO CONGRESS AND FEDERAL AGENCIES

SEC. 301. SENATE.

The Sergeant at Arms of the United States Senate shall develop regulations setting forth an information security and electronic privacy policy governing use of the Internet by officers and employees of the Senate that meets the requirements of title I.

SEC. 302. APPLICATION TO FEDERAL AGENCIES.

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

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

**TITLE IV—MISCELLANEOUS**

**SEC. 401. DEFINITIONS.**

In this Act:

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

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

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

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

(2) **COMMISSION.**—The term “Commission”
means the Federal Trade Commission.
(3) **COOKIE.**—The term “cookie” means any program, function, or device, commonly known as a “cookie”, that makes a record on the user’s computer (or other electronic device) of that user’s access to an internet service, online service, or commercial website.

(4) **DISCLOSE.**—The term “disclose” means the release of personally identifiable information about a user of an Internet service, online service, or commercial website by an internet service provider, online service provider, or operator of a commercial website for any purpose, except where such information is provided to a person who provides support for the internal operations of the service or website and who does not disclose or use that information for any other purpose.

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

(6) **INTERNAL OPERATIONS SUPPORT.**—The term “support for the internal operations of a service or website” means any activity necessary to maintain the technical functionality of that service or website.
(7) **INTERNET.**—The term “Internet” means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio.

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

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

(10) **OPERATOR OF A COMMERCIAL WEBSITE.**—The term “operator of a commercial website”—
(A) means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce—

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

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

(I) another such territory; or

(II) any State or foreign nation;

or

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

but

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

(11) PERSONALLY IDENTIFIABLE INFORMATION.—

(A) IN GENERAL.—The term "personally identifiable information" means individually identifiable information about an individual collected online, including—

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

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

(iii) an e-mail address;

(iv) a telephone number;

(v) a birth certificate number;

(vi) any other identifier for which the Commission finds there is a substantial likelihood that the identifier would permit the physical or online contacting of a specific individual; or

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

(B) **Inferential information excluded.**—Information about an individual derived or inferred from data collected online but not actually collected online is not personally identifiable information.

(12) **Release.**—The term “release of personally identifiable information” means the direct or indirect, sharing, selling, renting, or other provision of personally identifiable information of a user of an internet service, online service, or commercial website to any other person other than the user.

(13) **Robust notice.**—The term “robust notice” means actual notice at the point of collection of the personally identifiable information describing briefly and succinctly the intent of the Internet service provider, online service provider, or operator of a commercial website to use or disclose that information for marketing or other purposes.

(14) **Sensitive financial information.**—The term “sensitive financial information” means—

(A) the amount of income earned or losses suffered by an individual;
(B) an individual’s account number or balance information for a savings, checking, money market, credit card, brokerage, or other financial services account;

(C) the access code, security password, or similar mechanism that permits access to an individual’s financial services account;

(D) an individual’s insurance policy information, including the existence, premium, face amount, or coverage limits of an insurance policy held by or for the benefit of an individual; or

(E) an individual’s outstanding credit card, debt, or loan obligations.

(15) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term “sensitive personally identifiable information” means personally identifiable information about an individual’s—

(A) individually identifiable health information (as defined in section 164.501 of title 45, Code of Federal Regulations);

(B) race or ethnicity;

(C) political party affiliation;

(D) religious beliefs;

(E) sexual orientation;
40
(F) a Social Security number; or
(G) sensitive financial information.

SEC. 402. EFFECTIVE DATE OF TITLE I.

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

SEC. 403. FTC RULEMAKING.
The Commission shall—

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

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

SEC. 404. FTC REPORT.

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

(1) whether this Act is accomplishing the purposes for which it was enacted;

(2) whether technology that protects privacy is being utilized in the marketplace in such a manner as to facilitate administration of and compliance with title I;
(3) whether additional legislation is required to accomplish those purposes or improve the administrability or effectiveness of this Act;

(4) whether legislation is appropriate or necessary to regulate the collection, use, and distribution of personally identifiable information collected other than via the Internet;

(5) whether and how the government might assist industry in developing standard online privacy notices that substantially comply with the requirements of section 102(a);

(6) whether and how the creation of a set of self-regulatory guidelines established by independent safe harbor organizations and approved by the Commission would facilitate administration of and compliance with title I; and

(7) whether additional legislation is necessary or appropriate to regulate the collection, use, and disclosure of personally identifiable information collected online before the effective date of title I.

(b) FTC NOTICE OF INQUIRY.—The Commission shall initiate a notice of inquiry within 90 days after the date of enactment of this Act to request comment on the matter described in paragraphs (1) through (7) of subsection (a).
SEC. 405. DEVELOPMENT OF AUTOMATED PRIVACY CONTROLS.

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

(1) by redesignating subsection (d) as subsection (e); and

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

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