H. R. 29

To protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 4, 2005

Mrs. BONO (for herself, Mr. TOWNS, Mr. BARTON of Texas, Mr. BUYER, Mr. GILLMOR, Mr. HALL, Mr. RADANOVICH, Mr. WALDEN of Oregon, Mr. FERGUSON, Mr. WHITFIELD, Mrs. CUBIN, Mr. STEARNS, Mr. BILIRAKIS, Mr. TERRY, and Mr. OTTER) introduced the following bill; which was referred to the Committee on Energy and Commerce

A BILL

To protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purposes.

1 Be it enacted by the Senate and House of Representa-
2 tives of the United States of America in Congress assembled,

3 SECTION 1. SHORT TITLE.

4 This Act may be cited as the “Securely Protect Your-
5 self Against Cyber Trespass Act” or the “SPY ACT”.
SEC. 2. PROHIBITION OF DECEPTIVE ACTS OR PRACTICES RELATING TO SPYWARE.

(a) Prohibition.—It is unlawful for any person, who is not the owner or authorized user of a protected computer, to engage in deceptive acts or practices that involve any of the following conduct with respect to the protected computer:

(1) Taking control of the computer by—

(A) utilizing such computer to send unsolicited information or material from the protected computer to others;

(B) diverting the Internet browser of the computer, or similar program of the computer used to access and navigate the Internet—

(i) without authorization of the owner or authorized user of the computer; and

(ii) away from the site the user intended to view, to one or more other Web pages, such that the user is prevented from viewing the content at the intended Web page, unless such diverting is otherwise authorized;

(C) accessing or using the modem, or Internet connection or service, for the computer and thereby causing damage to the computer or
causing the owner or authorized user to incur unauthorized financial charges;

(D) using the computer as part of an activity performed by a group of computers that causes damage to another computer; or

(E) delivering advertisements that a user of the computer cannot close without turning off the computer or closing all sessions of the Internet browser for the computer.

(2) Modifying settings related to use of the computer or to the computer’s access to or use of the Internet by altering—

(A) the Web page that appears when the owner or authorized user launches an Internet browser or similar program used to access and navigate the Internet;

(B) the default provider used to access or search the Internet, or other existing Internet connections settings;

(C) a list of bookmarks used by the computer to access Web pages; or

(D) security or other settings of the computer that protect information about the owner or authorized user for the purposes of causing
damage or harm to the computer or owner or user.

(3) Collecting personally identifiable information through the use of a keystroke logging function.

(4) Inducing the owner or authorized user to install a computer software component onto the computer, or preventing reasonable efforts to block the installation or execution of, or to disable, a computer software component by—

(A) presenting the owner or authorized user with an option to decline installation of a software component such that, when the option is selected by the owner or authorized user, the installation nevertheless proceeds; or

(B) causing a computer software component that the owner or authorized user has properly removed or disabled to automatically reinstall or reactivate on the computer.

(5) Misrepresenting that installing a separate software component or providing log-in and password information is necessary for security or privacy reasons, or that installing a separate software component is necessary to open, view, or play a particular type of content.
(6) Inducing the owner or authorized user to install or execute computer software by misrepresenting the identity or authority of the person or entity providing the computer software to the owner or user.

(7) Inducing the owner or authorized user to provide personally identifiable, password, or account information to another person—

(A) by misrepresenting the identity of the person seeking the information; or

(B) without the authority of the intended recipient of the information.

(8) Removing, disabling, or rendering inoperative a security, anti-spyware, or anti-virus technology installed on the computer.

(9) Installing or executing on the computer one or more additional computer software components with the intent of causing a person to use such components in a way that violates any other provision of this section.

(b) GUIDANCE.—The Commission shall issue guidance regarding compliance with and violations of this section. This subsection shall take effect upon the date of the enactment of this Act.
(c) **Effective Date.**—Except as provided in subsection (b), this section shall take effect upon the expiration of the 6-month period that begins on the date of the enactment of this Act.

**SEC. 3. PROHIBITION OF COLLECTION OF CERTAIN INFORMATION WITHOUT NOTICE AND CONSENT.**

(a) **Opt-In Requirement.**—Except as provided in subsection (e), it is unlawful for any person—

(1) to transmit to a protected computer, which is not owned by such person and for which such person is not an authorized user, any information collection program, unless—

(A) such information collection program provides notice in accordance with subsection (c) before execution of any of the information collection functions of the program; and

(B) such information collection program includes the functions required under subsection (d); or

(2) to execute any information collection program installed on such a protected computer unless—

(A) before execution of any of the information collection functions of the program, the owner or an authorized user of the protected
computer has consented to such execution pursuant to notice in accordance with subsection (c); and

(B) such information collection program includes the functions required under subsection (d).

(b) INFORMATION COLLECTION PROGRAM.—For purposes of this section, the term “information collection program” means computer software that—

(1)(A) collects personally identifiable information; and

(B)(i) sends such information to a person other than the owner or authorized user of the computer, or

(ii) uses such information to deliver advertising to, or display advertising, on the computer; or

(2)(A) collects information regarding the Web pages accessed using the computer; and

(B) uses such information to deliver advertising to, or display advertising on, the computer.

(c) NOTICE AND CONSENT.—

(1) IN GENERAL.—Notice in accordance with this subsection with respect to an information collection program is clear and conspicuous notice in plain
language, set forth as the Commission shall provide, that meets all of the following requirements:

(A) The notice clearly distinguishes such notice from any other information visually presented contemporaneously on the protected computer.

(B) The notice contains one of the following statements, as applicable, or a substantially similar statement:

(i) With respect to an information collection program described in subsection (b)(1): “This program will collect and transmit information about you. Do you accept?”.

(ii) With respect to an information collection program described in subsection (b)(2): “This program will collect information about Web pages you access and will use that information to display advertising on your computer. Do you accept?”.

(iii) With respect to an information collection program that performs the actions described in both paragraphs (1) and (2) of subsection (b): “This program will collect and transmit information about you
and your computer use and will collect information about Web pages you access and use that information to display advertising on your computer. Do you accept?’’.

(C) The notice provides for the user—

(i) to grant or deny consent referred to in subsection (a) by selecting an option to grant or deny such consent; and

(ii) to abandon or cancel the transmission or execution referred to in subsection (a) without granting or denying such consent.

(D) The notice provides an option for the user to select to display on the computer, before granting or denying consent using the option required under subparagraph (C), a clear description of—

(i) the types of information to be collected and sent (if any) by the information collection program;

(ii) the purpose for which such information is to be collected and sent; and

(iii) in the case of an information collection program that first executes any of the information collection functions of the
program together with the first execution of other computer software, the identity of any such software that is an information collection program.

(E) The notice provides for concurrent display of the information required under subparagraphs (B) and (C) and the option required under subparagraph (D) until the user—

(i) grants or denies consent using the option required under subparagraph (C)(i);

(ii) abandons or cancels the transmission or execution pursuant to subparagraph (C)(ii); or

(ii) selects the option required under subparagraph (D).

(2) SINGLE NOTICE.—The Commission shall provide that, in the case in which multiple information collection programs are provided to the protected computer together, or as part of a suite of functionally-related software, the notice requirements of paragraphs (1)(A) and (2)(A) of subsection (a) may be met by providing, before execution of any of the information collection functions of the programs, clear and conspicuous notice in plain language in accordance with paragraph (1) of this sub-
section by means of a single notice that applies to all such information collection programs, except that such notice shall provide the option under subparagraph (D) of paragraph (1) of this subsection with respect to each such information collection program.

(3) Change in information collection.—If an owner or authorized user has granted consent to execution of an information collection program pursuant to a notice in accordance with this subsection:

(A) In general.—No subsequent such notice is required, except as provided in subparagraph (B).

(B) Subsequent notice.—The person who transmitted the program shall provide another notice in accordance with this subsection and obtain consent before such program may be used to collect or send information of a type or for a purpose that is materially different from, and outside the scope of, the type or purpose set forth in the initial or any previous notice.

(4) Regulations.—The Commission shall issue regulations to carry out this subsection.

(d) Required Functions.—The functions required under this subsection to be included in an information collection program that executes any information collection
functions with respect to a protected computer are as fol-

low:

(1) **DISABLING FUNCTION.**—With respect to any information collection program, a function of the program that allows a user of the program to remove the program or disable operation of the program with respect to such protected computer by a function that—

(A) is easily identifiable to a user of the computer; and

(B) can be performed without undue effort or knowledge by the user of the protected computer.

(2) **IDENTITY FUNCTION.**—With respect only to an information collection program that uses information collected in the manner described in paragraph (1)(B)(ii) or (2)(B) of subsection (b), a function of the program that provides that each display of an advertisement directed or displayed using such information when the owner or authorized user is accessing a Web page or online location other than of the provider of the software is accompanied by the name of the information collection program, a logogram or trademark used for the exclusive purpose of identi-
fying the program, or a statement or other informa-
tion sufficient to clearly identify the program.

(3) RULEMAKING.—The Commission may issue
regulations to carry out this subsection.

(e) LIMITATION ON LIABILITY.—A telecommuni-
cations carrier, a provider of information service or inter-
active computer service, a cable operator, or a provider
of transmission capability shall not be liable under this
section to the extent that the carrier, operator, or pro-
vider—

(1) transmits, routes, hosts, stores, or provides
connections for an information collection program
through a system or network controlled or operated
by or for the carrier, operator, or provider; or

(2) provides an information location tool, such
as a directory, index, reference, pointer, or hypertext
link, through which the owner or user of a protected
computer locates an information collection program.

SEC. 4. ENFORCEMENT.

(a) UNFAIR OR DECEPTIVE ACT OR PRACTICE.—
This Act shall be enforced by the Commission under the
A violation of any provision of this Act or of a regulation
issued under this Act committed with actual knowledge
or knowledge fairly implied on the basis of objective cir-
cumstances that such act is unfair or deceptive or violates this Act shall be treated as an unfair or deceptive act or practice violating a rule promulgated under section 18 of the Federal Trade Commission Act (15 U.S.C. 57a).

(b) PENALTY FOR PATTERN OR PRACTICE VIOLATIONS.—

(1) IN GENERAL.—Notwithstanding subsection (a) and the Federal Trade Commission Act, in the case of a person who engages in a pattern or practice that violates section 2 or 3, the Commission may, in its discretion, seek a civil penalty for such pattern or practice of violations in an amount, as determined by the Commission, of not more than—

(A) $3,000,000 for each violation of section 2; and

(B) $1,000,000 for each violation of section 3.

(2) TREATMENT OF SINGLE ACTION OR CONDUCT.—In applying paragraph (1)—

(A) any single action or conduct that violates section 2 or 3 with respect to multiple protected computers shall be treated as a single violation; and

(B) any single action or conduct that violates more than one paragraph of section 2(a)
shall be considered multiple violations, based on
the number of such paragraphs violated.

(c) EXCLUSIVENESS OF REMEDIES.—The remedies
in this section (including remedies available to the Com-
mission under the Federal Trade Commission Act) are the
exclusive remedies for violations of this Act.

(d) EFFECTIVE DATE.—This section shall take effect
on the date of the enactment of this Act, but only to the
extent that this section applies to violations of section
2(a).

SEC. 5. LIMITATIONS.

(a) LAW ENFORCEMENT AUTHORITY.—Sections 2
and 3 of this Act shall not apply to—

(1) any act taken by a law enforcement agent
in the performance of official duties; or

(2) the transmission or execution of an infor-
mation collection program in compliance with a law
enforcement, investigatory, national security, or reg-
ulatory agency or department of the United States
or any State in response to a request or demand
made under authority granted to that agency or de-
partment, including a warrant issued under the Fed-
eral Rules of Criminal Procedure, an equivalent
State warrant, a court order, or other lawful proc-
ess.
(b) EXCEPTION RELATING TO SECURITY.—Nothing in this Act shall apply to—

(1) any monitoring of, or interaction with, a subscriber’s Internet or other network connection or service, or a protected computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service, to the extent that such monitoring or interaction is for network or computer security purposes, diagnostics, technical support, or repair, or for the detection or prevention of fraudulent activities; or

(2) a discrete interaction with a protected computer by a provider of computer software solely to determine whether the user of the computer is authorized to use such software, that occurs upon—

(A) initialization of the software; or

(B) an affirmative request by the owner or authorized user for an update of, addition to, or technical service for, the software.

(c) GOOD SAMARITAN PROTECTION.—No provider of computer software or of interactive computer service may be held liable under this Act on account of any action voluntarily taken, or service provided, in good faith to remove or disable a program used to violate section 2 or 3 that
is installed on a computer of a customer of such provider,
if such provider notifies the customer and obtains the con-
sent of the customer before undertaking such action or
providing such service.

(d) LIMITATION ON LIABILITY.—A manufacturer or
retailer of computer equipment shall not be liable under
this Act to the extent that the manufacturer or retailer
is providing third party branded software that is installed
on the equipment the manufacturer or retailer is manufac-
turing or selling.

SEC. 6. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE LAW.—

(1) PREEMPTION OF SPYWARE LAWS.—This
Act supersedes any provision of a statute, regula-
tion, or rule of a State or political subdivision of a
State that expressly regulates—

(A) deceptive conduct with respect to com-
puters similar to that described in section 2(a);

(B) the transmission or execution of a
computer program similar to that described in
section 3; or

(C) the use of computer software that dis-
plays advertising content based on the Web
pages accessed using a computer.

(2) ADDITIONAL PREEMPTION.—
(A) IN GENERAL.—No person other than
the Attorney General of a State may bring a
civil action under the law of any State if such
action is premised in whole or in part upon the
defendant violating any provision of this Act.

(B) PROTECTION OF CONSUMER PROTEC-
tION LAWS.—This paragraph shall not be con-
strued to limit the enforcement of any State
consumer protection law by an Attorney Gen-
eral of a State.

(3) PROTECTION OF CERTAIN STATE LAWS.—
This Act shall not be construed to preempt the ap-
pliability of—

(A) State trespass, contract, or tort law; or

(B) other State laws to the extent that
those laws relate to acts of fraud.

(b) PRESERVATION OF FTC AUTHORITY.—Nothing
in this Act may be construed in any way to limit or affect
the Commission’s authority under any other provision of
law, including the authority to issue advisory opinions
(under Part 1 of Volume 16 of the Code of Federal Regu-
lations), policy statements, or guidance regarding this Act.

SEC. 7. ANNUAL FTC REPORT.

For the 12-month period that begins upon the effec-
tive date under section 11(a) and for each 12-month pe-
• HR 29 IH

period thereafter, the Commission shall submit a report to the Congress that—

(1) specifies the number and types of actions taken during such period to enforce sections 2(a) and 3, the disposition of each such action, any penalties levied in connection with such actions, and any penalties collected in connection with such actions; and

(2) describes the administrative structure and personnel and other resources committed by the Commission for enforcement of this Act during such period.

Each report under this subsection for a 12-month period shall be submitted not later than 90 days after the expiration of such period.

SEC. 8. FTC REPORT ON COOKIES.

(a) IN GENERAL.—Not later than the expiration of the 6-month period that begins on the date of the enactment of this Act, the Commission shall submit a report to the Congress regarding the use of tracking cookies in the delivery or display of advertising to the owners and users of computers. The report shall examine and describe the methods by which such tracking cookies and the websites that place them on computers function separately and together, and the extent to which they are covered
or affected by this Act. The report may include such recommendations as the Commission considers necessary and appropriate, including treatment of tracking cookies under this Act or other laws.

(b) DEFINITION.—For purposes of this section, the term “tracking cookie” means a cookie or similar text or data file used alone or in conjunction with one or more websites to transmit or convey personally identifiable information of a computer owner or user, or information regarding Web pages accessed by the owner or user, to a party other than the intended recipient, for the purpose of—

(1) delivering or displaying advertising to the owner or user; or

(2) assisting the intended recipient to deliver or display advertising to the owner, user, or others.

(c) EFFECTIVE DATE.—This section shall take effect on the date of the enactment of this Act.

SEC. 9. REGULATIONS.

(a) IN GENERAL.—The Commission shall issue the regulations required by this Act not later than the expiration of the 6-month period beginning on the date of the enactment of this Act. Any regulations issued pursuant to this Act shall be issued in accordance with section 553 of title 5, United States Code.
(b) EFFECTIVE DATE.—This section shall take effect on the date of the enactment of this Act.

SEC. 10. DEFINITIONS.

For purposes of this Act:

(1) CABLE OPERATOR.—The term “cable operator” has the meaning given such term in section 602 of the Communications Act of 1934 (47 U.S.C. 522).

(2) COLLECT.—The term “collect”, when used with respect to information and for purposes only of section 3, does not include obtaining of the information by a party who is intended by the owner or authorized user of a protected computer to receive the information pursuant to the owner or authorized user—

(A) transferring the information to such intended recipient using the protected computer; or

(B) storing the information on the protected computer in a manner so that it is accessible by such intended recipient.

(3) COMPUTER; PROTECTED COMPUTER.—The terms “computer” and “protected computer” have the meanings given such terms in section 1030(e) of title 18, United States Code.
(4) COMPUTER SOFTWARE.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term “computer software” means a set of statements or instructions that can be installed and executed on a computer for the purpose of bringing about a certain result.

(B) EXCEPTION FOR COOKIES.—Such term does not include—

(i) a cookie or other text or data file that is placed on the computer system of a user by an Internet service provider, interactive computer service, or Internet website to return information to such provider, service, or website; or

(ii) computer software that is placed on the computer system of a user by an Internet service provider, interactive computer service, or Internet website solely to enable the user subsequently to use such provider or service or to access such website.

(5) COMMISSION.—The term “Commission” means the Federal Trade Commission.
(6) DAMAGE.—The term “damage” has the meaning given such term in section 1030(e) of title 18, United States Code.

(7) DECEPTIVE ACTS OR PRACTICES.—The term “deceptive acts or practices” has the meaning applicable to such term for purposes of section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

(8) DISABLE.—The term “disable” means, with respect to an information collection program, to permanently prevent such program from executing any of the functions described in section 3(b) that such program is otherwise capable of executing (including by removing, deleting, or disabling the program), unless the owner or operator of a protected computer takes a subsequent affirmative action to enable the execution of such functions.

(9) INFORMATION COLLECTION FUNCTIONS.—The term “information collection functions” means, with respect to an information collection program, the functions of the program described in subsection (b) of section 3.

(10) INFORMATION SERVICE.—The term “information service” has the meaning given such term in section 3 of the Communications Act of 1934 (47 U.S.C. 153).
(11) **INTERACTIVE COMPUTER SERVICE.**—The term “interactive computer service” has the meaning given such term in section 230(f) of the Communications Act of 1934 (47 U.S.C. 230(f)).

(12) **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.

(13) **PERSONALLY IDENTIFIABLE INFORMATION.**—

(A) **IN GENERAL.**—The term “personally identifiable information” means the following information, to the extent only that such information allows a living individual to be identified from that information:

(i) First and last name of an individual.

(ii) A home or other physical address of an individual, including street name, name of a city or town, and zip code.
(iii) An electronic mail address.

(iv) A telephone number.

(v) A social security number, tax identification number, passport number, driver’s license number, or any other government-issued identification number.

(vi) A credit card number.

(vii) Any access code, password, or account number, other than an access code or password transmitted by an owner or authorized user of a protected computer to the intended recipient to register for, or log onto, a Web page or other Internet service or a network connection or service of a subscriber that is protected by an access code or password.

(viii) Date of birth, birth certificate number, or place of birth of an individual, except in the case of a date of birth transmitted or collected for the purpose of compliance with the law.

(B) RULEMAKING.—The Commission may, by regulation, add to the types of information specified under paragraph (1) that shall be considered personally identifiable information for
purposes of this Act, except that such informa-
tion may not include any record of aggregate
data that does not identify particular persons,
particular computers, particular users of com-
puters, or particular email addresses or other
locations of computers with respect to the
Internet.

(14) **Suite of functionally related software.**—The term ‘suite of functionally related software’
means a group of computer software programs dis-
tributed to an end user by a single provider, which
programs are necessary to enable features or
functionalities of an integrated service offered by the
provider.

(15) **Telecommunications carrier.**—The
term “telecommunications carrier” has the meaning
given such term in section 3 of the Communications

(16) **Transmit.**—The term “transmit” means,
with respect to an information collection program,
transmission by any means.

(17) **Web page.**—The term “Web page” means
a location, with respect to the World Wide Web, that
has a single Uniform Resource Locator or another
single location with respect to the Internet, as the Federal Trade Commission may prescribe.

SEC. 11. APPLICABILITY AND SUNSET.

(a) Effective Date.—Except as specifically provided otherwise in this Act, this Act shall take effect upon the expiration of the 12-month period that begins on the date of the enactment of this Act.

(b) Applicability.—Section 3 shall not apply to an information collection program installed on a protected computer before the effective date under subsection (a) of this section.

(c) Sunset.—This Act shall not apply after December 31, 2010.