

through 2009 to be devoted to prosecutions and expresses the sense of Congress that the Department of Justice should vigorously enforce the law against spyware violations as well as against online phishing scams in which criminals send fake e-mail messages to consumers on behalf of well-known companies and request account information that is later used to conduct criminal activities.

The bill also directs resources to the Department of Justice to combat pharming scams in which hackers intercept Internet traffic and redirect unknowing Internet users to fake Web sites where they often trick consumers into giving their account information and passwords.

I believe that four overarching principles should guide the consideration of any spyware legislation: first, we must punish the bad actors while protecting legitimate online companies; second, we must not overregulate but, rather, encourage innovative new services and the growth of the Internet; third, we must not stifle the free market; and, fourth, we must target the behavior, not the technology.

The targeted approach of the I-SPY Prevention Act will protect consumers by punishing the bad actors without imposing liability on those that act legitimately online. In addition, this legislation will avoid excessive regulation such as one-size-fits-all notice and consent requirements prescribed by the Federal Government. A targeted approach will avoid red tape that hampers the creation of new and exciting technologies and services on the Internet.

By encouraging innovation, the I-SPY Prevention Act will help ensure that consumers have access to cutting-edge products and services at lower prices. Increasingly, consumers want a seamless interaction with the Internet, and we must be careful to not interfere with businesses' ability to respond to this consumer demand with innovative services. The I-SPY Prevention Act will help ensure that consumers, not the Federal Government, define what their interaction with the Internet looks like.

As we move forward, I look forward to continuing to work with all stakeholders to further ensure that bad actors are punished while legitimate businesses are protected including working with the Department of Justice which has expressed an interest in working with our office on this issue. In addition, technological solutions are crucial in winning the fight against spyware. As the spyware debate continues, I look forward to working to ensure that antispymware technologies are fostered and that they are not subjected to frivolous lawsuits from spyware providers.

I urge my colleagues to support this important legislation.

Ms. ZOE LOFGREN of California. Mr. Speaker, I yield myself such time as I may consume.

I would just note that the House will be considering at least two items having to do with spamming and phishing and the like today. Certainly we hope to move this issue forward. I strongly believe that the approach that this bill takes, which is targeting behavior instead of technology, puts us on the soundest footing; and I hope that in the end as we sort through the various approaches that that will be our guide to protect technology innovation.

Ms. JACKSON-LEE of Texas. Mr. Speaker, I support the legislation before us that has been introduced by my colleague from California, Representative LOFGREN as well as the Gentleman from Virginia, Representative GOODLATTE. It amends the federal computer fraud and abuse statute to make it a clear offense to access a computer without authorization or to intentionally exceed authorized access by causing a computer program or code to be copied onto the computer and using that program or code to transmit or obtain personal information (for example, first and last names, addresses, e-mail addresses, telephone numbers, Social Security numbers, drivers license numbers, or bank or credit account numbers).

Furthermore, H.R. 744 authorizes appropriations for these crimes and discourages the practice of 'phishing.' As we all know too well, spyware is quickly becoming one of the biggest threats to consumers on the information superhighway. Spyware encompasses several potential risks including the promotion of identity theft by harvesting personal information from consumer's computers. Additionally, it can adversely affect businesses, as they are forced to sustain costs to block and remove spyware from employees' computers, in addition to the potential impact on productivity.

Spyware has been defined as "software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity with the consumer's consent, or asserts control over a computer with the consumer's knowledge." Among other things, criminals can use spyware to track every keystroke an individual makes, including credit card and social security numbers.

Some estimates suggest 25 percent of all personal computers contain some kind of spyware while other estimates show that spyware afflicts as many as 80-90 percent of all personal computers. Businesses are reporting several negative effects of spyware. Microsoft says evidence shows that spyware is "at least partially responsible for approximately one-half of all application crashes" reported to them, resulting in millions of dollars of unnecessary support calls.

Mr. Speaker, again, I am strongly in support of the legislation.

Ms. ZOE LOFGREN of California. Mr. Speaker, I yield back the balance of my time.

Mr. SENSENBRENNER. Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore (Mr. RADANOVICH). The question is on the motion offered by the gentleman from Wisconsin (Mr. SENSENBRENNER) that the House suspend the rules and pass the bill, H.R. 744, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds of

those present have voted in the affirmative.

Mr. SENSENBRENNER. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX and the Chair's prior announcement, further proceedings on this motion will be postponed.

#### SECURELY PROTECT YOURSELF AGAINST CYBER TRESPASS ACT

Mr. BARTON of Texas. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 29) to protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purposes, as amended.

The Clerk read as follows:

H.R. 29

*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 "Securely Protect Yourself Against Cyber Trespass Act" or the "Spy Act".

#### SEC. 2. PROHIBITION OF [UNFAIR OR] 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 unfair or 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 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, hijacking, or otherwise 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 or a third party defrauded by such conduct to incur charges or other costs for a service that is not authorized by such owner or authorized user;

(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 undue effort or knowledge by the user or 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 of the computer to disclose personally identifiable information by means of a Web page that—

(A) is substantially similar to a Web page established or provided by another person; and

(B) misleads the owner or authorized user that such Web page is provided by such other person.

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

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

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

(6) Misrepresenting that installing a separate component of computer software or providing log-in and password information is necessary for security or privacy reasons, or that installing a separate component of computer software is necessary to open, view, or play a particular type of content.

(7) 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.

(8) 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.

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

(10) Installing or executing on the computer one or more additional components of computer software 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.**—

(1) **IN GENERAL.**—For purposes of this section, the term “information collection program” means computer software that performs either of the following functions:

(A) **COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION.**—The computer software—

(i) collects personally identifiable information; and

(ii) (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.

(B) **COLLECTION OF INFORMATION REGARDING WEB PAGES VISITED TO DELIVER ADVERTISING.**—The computer software—

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

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

(2) **EXCEPTION FOR SOFTWARE COLLECTING INFORMATION REGARDING WEB PAGES VISITED WITHIN A PARTICULAR WEB SITE.**—Computer software that otherwise would be considered an information collection program by reason of paragraph (1)(B) shall not be considered such a program if—

(A) the only information collected by the software regarding Web pages that are accessed using the computer is information regarding Web pages within a particular Web site;

(B) such information collected is not sent to a person other than—

(i) the provider of the Web site accessed; or

(ii) a party authorized to facilitate the display or functionality of Web pages within the Web site accessed; and

(C) the only advertising delivered to or displayed on the computer using such information is advertising on Web pages within that particular Web site.

(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 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)(A): “This program will collect and transmit information about you. Do you accept?”

(ii) With respect to an information collection program described in subsection (b)(1)(B): “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 de-

scribed in both subparagraphs (A) and (B) of subsection (b)(1): “This program will collect and transmit information about you 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

(iii) 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 subsection 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 follows:

(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.**—

(A) **IN GENERAL.**—With respect only to an information collection program that uses information collected in the manner described in subparagraph (A)(ii)(II) or (B)(ii) of subsection (b)(1) and subject to subparagraph (B) of this paragraph, 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 computer software, is accompanied by the name of the information collection program, a logogram or trademark used for the exclusive purpose of identifying the program, or a statement or other information sufficient to clearly identify the program.

(B) **EXEMPTION FOR EMBEDDED ADVERTISEMENTS.**—The Commission shall, by regulation, exempt from the applicability of subparagraph (A) the embedded display of any advertisement on a Web page that contemporaneously displays other information.

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

(e) **LIMITATION ON LIABILITY.**—A telecommunications carrier, a provider of information service or interactive 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 provider—

(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 Federal Trade Commission Act (15 U.S.C. 41 et seq.). A violation of any provision of this Act or of a regulation issued under 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) **REQUIRED SCIENTER.**—Civil penalties sought under this section for any action may not be granted by the Commission or any court unless the Commission or court, respectively, establishes that the action was committed with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive or violates this Act.

(d) **FACTORS IN AMOUNT OF PENALTY.**—In determining the amount of any penalty pursuant to subsection (a) or (b), the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require.

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

(f) **EFFECTIVE DATE.**—To the extent only that this section applies to violations of section 2(a), 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. 5. LIMITATIONS.

(a) **LAW ENFORCEMENT AUTHORITY.**—Sections 2 and 3 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 information collection program in compliance with a law enforcement, investigatory, national security, or regulatory 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 department, including a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a court order, or other lawful process.

(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 consent 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 computer software that is installed on the equipment the manufacturer or retailer is manufacturing 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, regulation, or rule of a State or political subdivision of a State that expressly regulates—

(A) unfair or deceptive conduct with respect to computers 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 displays 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 PROTECTION LAWS.**—This paragraph shall not be construed to limit the enforcement of any State consumer protection law by an Attorney General of a State.

(3) **PROTECTION OF CERTAIN STATE LAWS.**—This Act shall not be construed to preempt the applicability 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 Regulations), policy statements, or guidance regarding this Act.

#### SEC. 7. ANNUAL FTC REPORT.

For the 12-month period that begins upon the effective date under section 12(a) and for each 12-month 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 section 2(a) and section 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 cookies, including 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 cookies and the Web sites that place them on computers function separately and together, and shall compare the use of cookies with the use of information collection programs (as such term is defined in section 3) to determine the extent to which such uses are similar or different. The report may include such recommendations as the Commission considers

necessary and appropriate, including treatment of 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 Web sites to transmit or convey, to a party other than the intended recipient, personally identifiable information of a computer owner or user, information regarding Web pages accessed by the owner or user, or information regarding advertisements previously delivered to a computer, 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. FTC REPORT ON INFORMATION COLLECTION PROGRAMS INSTALLED BEFORE EFFECTIVE DATE.**

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 on the extent to which there are installed on protected computers information collection programs that, but for installation prior to the effective date under section 12(a), would be subject to the requirements of section 3. The report shall include recommendations regarding the means of affording computer users affected by such information collection programs the protections of section 3, including recommendations regarding requiring a one-time notice and consent by the owner or authorized user of a computer to the continued collection of information by such a program so installed on the computer.

**SEC. 10. 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. In exercising its authority to issue any regulation under this Act, the Commission shall determine that the regulation is consistent with the public interest and the purposes 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. 11. 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(b)(1)(A), 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 or by a third party authorized by such intended recipient 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 soft-

ware” 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.—Such term does not include computer software that is placed on the computer system of a user by an Internet service provider, interactive computer service, or Internet Web site solely to enable the user subsequently to use such provider or service or to access such Web site.

(C) RULE OF CONSTRUCTION REGARDING COOKIES.—This paragraph may not be construed to include, as computer software—

(i) a cookie; or

(ii) any other type of text or data file that solely may be read or transferred by a computer.

(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)(1) 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)(1) 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 described in subparagraph (A) that shall be considered personally identifiable information for purposes of this Act, except that such additional types of information shall be considered personally identifiable information only to the extent that such information allows living individuals, particular computers, particular users of computers, or particular email addresses or other locations of computers to be identified from that information.

(14) SUITE OF FUNCTIONALLY RELATED SOFTWARE.—The term suite of “functionally related software” means a group of computer software programs distributed 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 Act of 1934 (47 U.S.C. 153).

(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.

(18) WEB SITE.—The term “web site” means a collection of Web pages that are presented and made available by means of the World Wide Web as a single Web site (or a single Web page so presented and made available), which Web pages have any of the following characteristics:

(A) A common domain name.

(B) Common ownership, management, or registration.

**SEC. 12. 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, 2011.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Texas (Mr. BARTON) and the gentlewoman from Illinois (Ms. SCHAKOWSKY) each will control 20 minutes.

The Chair recognizes the gentleman from Texas (Mr. BARTON).

GENERAL LEAVE

Mr. BARTON of Texas. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks on this legislation and insert extraneous material in the RECORD.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Texas?

There was no objection.

Mr. BARTON of Texas. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, today the House will consider legislation to prohibit Internet spying. Spyware is a growing danger to Internet users and one that demands our immediate attention. Recent statistics indicate that spyware is on the rise, with the highest areas of growth in Trojans, keystroke loggers and system monitors, the worst-of-the-worst spyware technologies.

The Committee on Energy and Commerce has worked expeditiously this Congress to move antispyware legislation through the committee for consideration by the House. This legislation is largely the same as H.R. 2929 from the 108th Congress, a bill that passed the House by a vote of 399-1. It is my hope that H.R. 29 will receive a similar endorsement today on this floor.

The changes that have been made to the SPY ACT since the last Congress are of two general types. The Committee on Energy and Commerce worked hard to refine the legislation to take into account legitimate and benign business functions, as well as standard functionalities of the Internet while preserving meaningful consumer notice and consent. The committee has also continued to strengthen the anti-fraud provisions of the bill by giving the Federal Trade Commission better enforcement tools against the ever-increasing types of fraudulent behavior associated with Internet spying.

The legislation that we are considering today, number one, prohibits unfair and deceptive practices like home page hijacking, keystroke logging, and Web-based phishing; two, provides for a prominent opt-in for consumers prior to the collection of personally identifiable information by monitoring spyware. This is a very, very important provision of the bill. Three, provides for a prominent opt-in for consumers prior to the collection of information regarding Web pages accessed and the subsequent delivery of advertisements based on that information; four, requires that monitoring software be easily disabled at the direction of the consumer; five, requires companies that are sending ads to computers to identify with each ad the information collection program that is generating the ad. With this disclosure, consumers will know who is bombarding them with ads and will be able to make decisions about those pieces of software accordingly. Number six, provides for FTC enforcement with significant monetary penalties for those who knowingly violate the act; and, seven, sets up a uniform national rule. Internet commerce is inherently interstate in nature. We need one set of rules for such commerce, not 50.

We have just today also passed a bill that makes explicit some criminal penalties for purveyors of the worst kinds of spyware. I think it is appropriate that in certain instances, such as deceptive phishing leading to identity theft, the perpetrators need to go to jail. I want to thank the Committee on the Judiciary for their work in that

area. However, I believe we need to do more to protect consumers. I believe we need to recognize the right of each consumer to be informed of spying taking place on his or her computer and be able to say no to that spying. This bill does that. The bill that we just passed from the Committee on the Judiciary does not do that.

I believe that we need to require of ad companies the responsibility to inform consumers and to get their consent before they start installing devices on consumers' computers that keep track of everything that they do, and their children do, on the Internet. This bill does that. The bill from the Committee on the Judiciary does not do that.

And I believe that companies have an obligation to disable spying programs if the consumers no longer want them. A consumer should have more options than just throwing away his computer if it is infected with spyware. This bill does that. The bill that came out of the Committee on the Judiciary does not do that.

It is this empowerment of consumers and the recognition that each consumer has the right to control what goes on his or her own computer that makes this bill, H.R. 29, a very important tool to protect consumers against spyware. That consumer protection will be my goal when we go to conference with the Senate.

I want to commend a number of Members for their outstanding leadership on this issue. The gentlewoman from California (Mrs. BONO) who will speak later in the debated introduced the original bill in the last Congress and has been a tireless educator on the dangers of spyware. The gentleman from New York (Mr. TOWNS) cosponsored the original legislation with the gentlewoman from California (Mrs. BONO), and he has been great in his bipartisan support of this particular project. The gentleman from Florida (Mr. STEARNS), the chairman of the Subcommittee on Trade and Consumer Protection, has been a leader on all the privacy-related issues in the committee and has worked with the gentlewoman from California (Mrs. BONO) and the gentleman from New York (Mr. TOWNS) on this legislation.

The gentleman from Michigan (Mr. DINGELL), the ranking member of the full committee, and the gentlewoman from Illinois (Ms. SCHAKOWSKY), who is leading the floor debate on the Democratic side, have worked tirelessly in both the subcommittee and the full committee to perfect this bipartisan legislation.

This is a good bill. It is a bipartisan bill. It passed the Committee on Energy and Commerce unanimously. I would urge that it pass the floor later this afternoon with that same level of support.

Mr. Speaker, I reserve the balance of my time.

Ms. SCHAKOWSKY. Mr. Speaker, I yield myself such time as I may consume.

I rise today as a cosponsor and in support of a strong consumer and privacy protection bill, H.R. 29, the Securely Protect Yourself Against Cyber Trespass Act, or the SPY ACT. I want to thank the gentleman from Texas (Mr. BARTON), the gentleman from Michigan (Mr. DINGELL), the gentleman from Florida (Mr. STEARNS), the gentleman from New York (Mr. TOWNS), and the gentlewoman from California (Mrs. BONO) for their work on the SPY ACT.

I would like first to commend the manner in which this bill was handled. The process was thorough, open to input and willing to address each other's concerns; and, most importantly, the work was organized around the goal of creating a strong and effective consumer protection bill. I believe we have accomplished our goal.

Spyware is software that has tracking capabilities so pervasive that it can record every keystroke computer users enter. It can take pictures of personal computer screens. It can snatch personal information from consumers' hard drives. People can see their bank account numbers, passwords, and other personal information stolen because they quite innocently went to a bad Web site or clicked a misleading agreement. Spyware is a serious threat to consumer privacy and potentially a powerful tool for identity theft, a serious crime that is on the rise. Spyware is a nonpartisan issue. As we learned last year while not yet a household word, spyware is a household phenomenon.

□ 1445

America Online recently released a study which found that 80 percent of families with broadband access had spyware on their computers. Earthlink found that in 3 million scans of computers, there was an average of 26 instances of spyware on each and every computer. With those kinds of numbers, spyware will soon be a part of everyone's vocabulary.

Technological advances have brought "the world into our homes," and the purveyors of spyware have interpreted that as an open door to come in whenever they want, whether invited or not. Still, because the software does have shady purposes, it usually comes in through the back door of consumers' computers. Because consumers do not know that spyware is on their computers, people are still surprised to hear about it. They experience the noticeable effects of the software, impossibly slow computers, hijacked home pages, unstoppable pop-ups, but they do not know where their problems are coming from or what is going on behind the scenes.

For instance, someone's computer may be sluggish because she may unwittingly have downloaded a program that records every key stroke entered and passes it on to a third party who wants to steal bank account numbers and passwords. The explosion of pop-up

ads may be because a program has been tracking a consumer's every move on the Web. Serious privacy and security issues are at stake here. Spyware could be a major contributor to the fact that identity theft is the fastest-growing financial crime today.

The time has come for a bill like the Spy Act. The gentleman from Texas (Chairman BARTON) very clearly outlined the specific provisions of the bill, but it bears briefly repeating. The Spy Act ensures that consumers are protected from the truly bad acts and actors while also protecting proconsumer functions of the software. It prohibits indefensible uses of the software like keystroke logging or the copying of every keystroke entered. Additionally, it gives the consumer the choice to opt in to the installation or activation of information collection programs on their computers, but only when they know exactly what information will be collected and what will be done with it. Furthermore, the Spy Act gives the Federal Trade Commission the power it needs on top of laws already in place to pursue deceptive uses of the software. The Spy Act puts the control of computers and privacy back in consumers' hands, and I am very glad I was a part of the process that brought this bill to the floor today.

So, again, I thank my colleagues for their work on this proconsumer, proprivacy, and bipartisan legislation, and I urge all Members to support it.

Mr. Speaker, I reserve the balance of my time.

Mr. BARTON of Texas. Mr. Speaker, I yield 5 minutes to the gentleman from Florida (Mr. STEARNS), subcommittee chairman.

(Mr. STEARNS asked and was given permission to revise and extend his remarks.)

Mr. STEARNS. Mr. Speaker, I thank the gentleman from Texas (Mr. BARTON), my distinguished chairman of the full committee, for yielding me this time.

This is a very important bill. We have passed this bill once before, so it is clear the House is going to pass this. The question is, we have got to appeal to the Senate to pass this thing and move forward.

During the hearings we had on this bill, there were lots of witnesses that talked about this spyware Internet-based technology that can be used to defraud Americans today. So this bill is very important. We need to move it, and we need to move the Senate to move it. That is what we need to do.

This bill describes a broad array of activity, including keystroke logging, which tracks all of a computer user's keystrokes, they are recorded and then sent to a third party; homepage hijacking, in which spyware can take control of a computer and hijack the user's homepage to a commercial site or even to a pornographic site; and phishing, in which spyware directs a computer user with false messages purporting to be from some reputable merchant to basi-

cally steal the credit card, steal the credit card numbers and other financial information from a user.

In all of these cases, Mr. Speaker, spyware is downloaded without the knowledge and without the consent of the user. It is just not another cyber nuisance. It is a major Internet plague that threatens the privacy of the American consumer, and of course the very integrity of the Internet marketplace, on which we are relying more and more. I continue to meet people who have had their Web pages hijacked, their browsers corrupted, in some cases, their children exposed to inappropriate material from these dangerous programs hidden in their family computers.

Mr. Speaker, the Spy Act will bring control back to the consumer and give the on-line computer experience a positive message. It will preserve confidence in the Internet and its related technologies that make the lives of the consumer better and more convenient, more productive, and, of course, more secure. The Spy Act strikes a right balance between preserving legitimate and benign uses of this technology, while still, at the same time, protecting unwitting consumers from the harm caused when it is misused and, of course, designed for nefarious purposes.

The Spy Act prohibits keystroke logging, hijacking, and phishing. I mentioned that. It also provides a well-crafted opt-in for consumers before personal information is collected or prior to collection of Web history information. We in the Committee on Energy and Commerce think that is extremely important to have an opt-in for consumers. The legislation specifies that monitoring software should be easily disabled and requires companies that deliver ads to simply identify themselves. Further and more importantly, it gives the Federal Trade Commission the power to severely sanction violators with significant monetary penalties. In short, Mr. Speaker, this legislation creates a uniform Federal regulatory regime that will provide clear and consistent regulation in this area.

At the bottom, the elimination of spyware and the preservation of privacy for the consumer are critical goals if the Internet is to remain safe and reliable and credible.

As I mentioned earlier, the House passed the bill H.R. 2929 by a vote of 399 to 1. This year this legislation was passed unanimously out of the Committee on Energy and Commerce, 43 to zero. I expect the same strong showing this afternoon.

So, in conclusion, Mr. Speaker, H.R. 29, the Spy Act, has been a great exercise, as mentioned by the gentleman from Illinois (Ms. SCHAKOWSKY), ranking member, of our bipartisan leadership. Leadership that has been focused on achieving equitable results, that is good for the consumer, good for business, and good for America.

With that in mind, I would like to thank my colleagues on the Committee

on Energy and Commerce, particularly the gentleman from Texas (Chairman BARTON) and the gentlewoman from California (Mrs. BONO), whose leadership provided this bill, for their consistent and, of course, their longstanding leadership in this area. I would also like to acknowledge the superb bipartisanship of my staff working with the staff of the gentlewoman from Illinois (Ms. SCHAKOWSKY).

And, of course, I would also like to thank the gentleman from Michigan (Mr. DINGELL), the ranking member of the full committee, and the gentleman from New York (Mr. TOWNS) for his support.

So, all in all, Mr. Speaker, we have a great bill. We need to move the Senate forward. Our bill will make America greater, and I urge support for the Spy Act of 2005.

Ms. SCHAKOWSKY. Mr. Speaker, I yield myself such time as I may consume.

I can only heartily agree with all that has been said. Let me just add a few words.

Spyware has changed the computing experience for so many people. Increasingly, consumers are finding that their home Web pages are changed or that their computers are sluggish; and they get, as I said, the pop-up ads that will not go away no matter how many times they try to close them. They find software in their computer they did not install and they cannot uninstall; and their computers are no longer their own, and they cannot figure out why. And consumers tend to blame viruses on their old computer or their Internet service providers, but because spyware is bundled with software people do want to download or because it is drive-by downloaded from unknowingly visiting the wrong Web site, people do not know that in many cases the real cause of their headaches is spyware.

And some of the above examples can be written off as merely annoying. Spyware is so much more than merely annoying, as we have pointed out, and there are these serious privacy and security issues at stake.

These problems of slow computers and pop-up ads are just symptoms of the real trouble spyware can cause. Again, the software is so resourceful that it can snatch personal information from computer hard drives and track every Web site visited and log every keystroke entered.

Spyware is a serious threat to consumer privacy and potentially a powerful tool for identity theft, a serious crime on the rise. As the FTC, the Federal Trade Commission, reports, in 2003 there were nearly 10 million Americans victimized by identity theft. Over the past 5 years, there have been 27 million victims, and my State of Illinois is in the top 10 for identity theft occurrences. On-line predators, like spyware transmitters, provide an easy access to personally identifiable information that can be used to steal people's identities and put them at greater risk of

being financially and otherwise victimized.

So this is now the time, once again, for the House to pass this important bipartisan legislation. And I too want to thank all of the leaders who have been involved in bringing this bill once again to the floor. I want to particularly thank the gentleman from Michigan (Mr. DINGELL), whose statement, though he could not be here today, will be in the RECORD, and the gentleman from New York (Mr. TOWNS), who has worked on this legislation from the very beginning with the gentlewoman from California (Mrs. BONO). And I want to thank the staff on our side, Diane Beedle and Consuela Washington, and the Republican staff for their hours of work.

I want to join the gentleman from Florida (Chairman STEARNS) in urging our Senate colleagues to move on this very important legislation. It is time that we not only pass it in the House, but that we make it the law of the land, and I look forward to seeing that happen in the near future. I thank my colleagues for the opportunity to work with all of them.

Mr. Speaker, I have no further requests for time, and I yield back the balance of my time.

Mr. BARTON of Texas. Mr. Speaker, I yield 5 minutes to the distinguished gentlewoman from Palm Springs, California (Mrs. BONO), the author of the original bill, who knows more about these types of issues than anybody on the committee.

Mrs. BONO. Mr. Speaker, I want to thank the gentleman from Texas for yielding me this time.

The gentleman from Texas (Chairman BARTON) has been a steadfast leader and advocate for spyware legislation. He has worked tirelessly on this important issue. I appreciate his efforts in bringing H.R. 29 to the floor. I also extend my appreciation to the gentleman from Michigan (Mr. DINGELL), ranking member; the gentleman from Florida (Chairman STEARNS); the gentlewoman from Illinois (Ms. SCHAKOWSKY), ranking member; and the gentleman from New York (Mr. TOWNS), the original Democratic cosponsor. Each of them, as well as their staff, David Cavicke, Shannon Jacquot, Consuela Washington, Chris Leahy, Diane Beedle, Andy Delia, Dave Grimaldi; as well as my staffers, Jennifer Baird and Chris Lynch, have all worked diligently over the past 2 years to improve and refine this legislation.

I would also like to thank the industry participants and consumer groups who have contributed hundreds of comments on this legislation. I am confident that we have drafted a bill that incorporates several improvements that will empower consumers without impeding the growth of technology or on-line business models.

In the wake of recent data security breaches by ChoicePoint, DSW, Lexis-Nexis, and other companies, consumers are finally realizing the importance of

data security and their vulnerability to identity theft. While consumers are waking up to these risks, many continue to remain unaware of the consequences of having spyware programs on their computers. Spyware is software that is downloaded on one's computer that collects personally identifiable information such as Social Security numbers, credit card numbers, addresses, and phone numbers. This software passes personal information on to third parties without consent, or it is used to drive advertising to their computer. In short, it compromises personal data and can physically harm their computer.

Just how prolific is this problem? Here are a few of the staggering statistics: In a recent study by Webroot, the company identified at least one form of an unwanted program in 87 percent of the personal computers it scanned. Results from a consumer spy audit in 2005 found that 88 percent of personal computers scanned were infected with an average of 25 different spyware programs in each computer. In March, 2005, alone, a research system identified over 4,000 Web sites within nearly 90,000 total associated Web pages containing some form of spyware. Trojan horse infections grew by 30 percent since last year.

□ 1500

Mr. Speaker, this is not just a problem; it is an outright epidemic. As this Nation continues to push towards a global e-commerce marketplace, spyware stands to undermine the security and integrity of e-commerce and data security. Daily Web activities by consumers have become stalking grounds for computer hackers through spyware.

Consumers regularly and unknowingly download software programs that have the ability to track their every move. While some argue that consumers consented to these spyware downloads, the National Cyber Security Alliance and AOL found that 89 percent of users had no idea they had spyware on their computers. Moreover, there are Web sites and e-mail messages that deliberately trick computer users into downloading spyware.

In response to the rapid proliferation of spyware, the gentleman from New York (Mr. TOWNS) and I introduced H.R. 29. This bill prohibits such behavior by specifically outlawing Web hijacking, keystroke logging, drive-by downloads, phishing, evil-twin attacks and, several other perverse behaviors.

The concept of H.R. 29 is simple: tell consumers in plain English what personally identifiable information is going to be collected and how that information is going to be used. Consumers have a right to know and have a right to decide who has access to such highly personal information. Therefore, it is imperative that Congress pass this legislation and empower consumers while not impeding the growth of technology.

Earlier we heard my colleagues from the Committee on the Judiciary bring up their bill and talk about targeting behavior and not technology. I would ask them, what is Kazaa? Is Kazaa behavior or technology? What is Bonzi Buddy? Bonzi Buddy downloads a beautiful little purple gorilla which will dance about your screen which you cannot possibly eradicate from your computer. What is the Weather Bug? Again, the Committee on the Judiciary would say this is simply technology. I disagree. I say it is a terrible, terrible business practice, and it needs to be recognized by Congress. We need to stamp this out.

Mr. Speaker, I urge my colleagues to support H.R. 29.

Mr. BARTON of Texas. Mr. Speaker, I yield myself the balance of my time to close.

Mr. Speaker, I would like to read into the RECORD the companies and the organizations that support H.R. 29. This is with letters on the RECORD where they have written to me and the gentleman from Michigan (Mr. DINGELL) that they support the legislation: the Business Software Alliance; the Center For Democracy and Technology; the Council For Marketing and Opinion Research; Dell Corporation; DoubleClick, Incorporated, and ValueClick, Incorporated; eBay, Incorporated; Fidelity; Humana, Incorporated; Microsoft; 180 Solutions; the Recording Industry of America; Time Warner/AOL; United States Telecom Association; Webroot Software, Incorporated; WhenU; and Yahoo. These companies all officially on the record support H.R. 29.

Mr. Speaker, I think as the debate has shown, there is broad bipartisan support for this. There is also a need for this. I have spoken with Senator BURNS of the other body. He is preparing to move a companion bill. We have also obviously talked to the gentleman from Wisconsin (Chairman SENSENBRENNER) and the subcommittee chairman, the gentleman from Virginia (Mr. GOODLATTE), on their bill; and we are prepared to work with them to merge the bills at the appropriate time.

This is an issue whose time has come. Almost every American household now has a personal computer, and almost every one of those computers has spyware on them; and in most cases the owner of that computer does not know it. It is time to put a stop to that foolishness. It is time to say enough is enough. It is time to pass H.R. 29, work with the other body to pass a companion bill, go to conference, create a compromise bill, and then send the bill to the President's desk.

So I would encourage a "yes" vote, Mr. Speaker, and before I yield back, compliment you on your work on this. I think we should say the gentleman from California (Mr. RADANOVICH) also has been tireless in his support for the bill.

Mr. DINGELL. Mr. Speaker, identity theft is fast reaching epidemic proportions. Today we

will address one aspect of the problem—spyware.

Spyware programs sneak into your computer, and allow a third party to harvest your personal information. It is the equivalent of putting a wiretap on your phone and listening to your conversations. Adware tracks your Web surfing or online shopping so that marketers can send you unwanted ads. Spyware can hijack your computer to pornographic or gambling sites, or steal your passwords and credit card information.

The rapid proliferation of spyware and adware threatens legitimate Internet commerce. The most common consumer complaints are: hijacked home pages, redirected Web searches, a flood of pop-up ads, and sluggish and crashed computers.

This bill is carefully balanced. It prohibits a number of unfair and deceptive acts or practices related to spyware, and provides for strong Federal Trade Commission (FTC) enforcement and enhanced civil fines. It also recognizes that there are legitimate, applications of spyware and, thus, exempts law enforcement, national security, network security and maintenance, and fraud detection from the SPY Act. It contains narrowly prescribed exceptions for benign internal navigation tracking on Web sites, and the ordinary construction of Web pages that do not collect personal information. It preserves legitimate online commerce.

Most importantly, this legislation requires companies that distribute spyware and adware to obtain permission from consumers through an easily understood licensing agreement before installing spyware or adware on their computers. The programs, once downloaded, would have to provide a means to identify the spyware or adware and easily uninstall or disable it.

Without aggressive enforcement, the goals of this bill will not be met. We are asking the FTC to do a great deal in a very complex area and I trust that the appropriators will provide them with sufficient resources to fulfill these tasks. If not, this bill will be an empty promise, unless the state attorneys general step in forcefully.

This legislation is supported by a coalition that includes: the Business Software Alliance, the Center for Democracy and Technology, the Council for Marketing and Opinion Research, Dell, eBay Inc., Fidelity, Humana, Inc., Microsoft, 180 Solutions, Recording Industry Association of America, Time Warner/AOL, United States Telecom Association, Webroot Software, Inc., WhenU, and Yahoo!—all of whom have submitted letters of support. The coalition also includes DoubleClick, Inc., and ValueClick, Inc.—two of the leading companies in the rapidly growing online advertising industry.

The bill has improved at every stage of its consideration, and I want to commend the leadership and hard work of Chairman BARTON, Representatives STEARNS and SCHAKOWSKY, the Chairman and Ranking Member, respectively of the Subcommittee on Commerce, Trade, and Consumer Protection, and Representatives BONO and TOWNS, the lead Republican and Democratic sponsors of the bill. I also commend the bipartisan staff team who worked very hard to get this bill to the House floor.

I am proud to cosponsor this bill. I urge my colleagues to vote "yes" on passage of H.R.

29. It is a good bill. It is good for consumers. And it is good for honest commerce on the Internet.

Mr. BARTON of Texas. Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore (Mr. RADANOVICH). The question is on the motion offered by the gentleman from Texas (Mr. BARTON) that the House suspend the rules and pass the bill, H.R. 29, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds of those present have voted in the affirmative.

Mr. BARTON of Texas. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX and the Chair's prior announcement, further proceedings on this motion will be postponed.

#### HEROES EARNED RETIREMENT OPPORTUNITIES ACT

Mr. SAM JOHNSON of Texas. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 1499) to amend the Internal Revenue Code of 1986 to allow a deduction to members of the Armed Forces serving in a combat zone for contributions to their individual retirement plans even if the compensation on which such contribution is based is excluded from gross income, and for other purposes, as amended.

The Clerk read as follows:

H.R. 1499

*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 "Heroes Earned Retirement Opportunities Act".

##### SEC. 2. COMBAT ZONE COMPENSATION TAKEN INTO ACCOUNT FOR PURPOSES OF DETERMINING LIMITATION AND DEDUCTIBILITY OF CONTRIBUTIONS TO INDIVIDUAL RETIREMENT PLANS.

(a) IN GENERAL.—Subsection (f) of section 219 of the Internal Revenue Code of 1986 is amended by redesignating paragraph (7) as paragraph (8) and by inserting after paragraph (6) the following new paragraph:

"(7) SPECIAL RULE FOR COMPENSATION EARNED BY MEMBERS OF THE ARMED FORCES FOR SERVICE IN A COMBAT ZONE.—For purposes of subsections (b)(1)(B) and (c), the amount of compensation includible in an individual's gross income shall be determined without regard to section 112."

(b) EFFECTIVE DATE.—The amendments made by this section shall apply to taxable years beginning after December 31, 2004.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Texas (Mr. SAM JOHNSON) and the gentleman from Michigan (Mr. LEVIN) each will control 20 minutes.

The Chair recognizes the gentleman from Texas (Mr. SAM JOHNSON).

##### GENERAL LEAVE

Mr. SAM JOHNSON of Texas. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend

their remarks and include extraneous material on H.R. 1499.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Texas?

There was no objection.

Mr. SAM JOHNSON of Texas. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in support of backing our troops, of backing them to the hilt, with the Heroes Earned Retirement Opportunities Act, or the HERO Act, H.R. 1499, introduced by the gentlewoman from North Carolina (Ms. FOX).

As you know, people may contribute to \$4,000 a year to the popular individual retirement account, IRA. However, the funds that go into an IRA are supposed to be post-tax money. Well, when you are serving your country in Camp Victory in Iraq or working in Afghanistan, your combat pay is tax-free. That is right, it is tax-free; and it ought to be. The theory behind that is if you are going to volunteer to risk your life, serve your country and protect our great freedom, you should not be taxed.

As a result, some military men and women come home serving in harm's way with money that they would like to put into an individual retirement account, but they cannot. It is against the law. That is wrong. The HERO Act changes that outdated and unintended tax law so that our soldiers, sailors, Marines and airmen can save some of that money for their retirement for their families' golden years.

Crazy as it may seem, right now these men and women come home with much more disposable income, yet they are not allowed to save some of it in an IRA; but they can spend it on cars, new clothes, family vacations. Yes, all of those things are nice, especially when you have been in the desert for 9 months and you just want the creature comforts and luxuries of home for you and your family. But those things are temporary. Retirement savings is about making a better future for yourself and your loved ones, and our troops should have the option of saving for retirement if they want to.

I say it is high time we change that, and that is what the HERO Act is all about. It is about tax simplification, it is about retirement savings, it is about helping our military who are out there fighting for us.

Mr. Speaker, I reserve the balance of my time.

Mr. LEVIN. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I stand today in support of H.R. 1499. This bill is supported by my Democratic colleagues. We acknowledge fully the work of our military personnel who continue to perform for our Nation. We honor their bravery and their sacrifice. Therefore, it goes without saying that we endorse this effort by this Congress to make it possible for these men and women to take advantage of every tax benefit