mammography equipment to the National Mammography Quality Assurance Advisory Committee and grants the advisory committee greater flexibility in how many times the committee must meet annually.

Mr. Speaker, this is a good piece of legislation and I would encourage my colleagues to support it.

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

Mr. BROWN of Ohio. Mr. Speaker, I yield myself 3 minutes.

Mr. Speaker, I would like to thank the gentleman from Texas (Chairman BARTON) for his good work on this legislation, the gentleman from Michigan (Mr. DINGELL) and the gentleman from Florida (Chairman BILIRAKIS) for offering this legislation reauthorizing the Mammography Quality Standards Act of 1992.

The gentleman from Michigan (Mr. DINGELL) pioneered this important legislation a dozen years or so ago. By increasing the breast cancer early detection rate, this legislation has undoubtedly contributed to the battle against this deadly disease.

Breast cancer is the top cancer threat for American women. This year alone, in our country, almost 216,000 women will be diagnosed with breast cancer, and more than 40,000 will lose their lives from it.

Accurate reading of mammograms is essential to early detection of breast cancer. Mammography has increased the survival rate for women in their 40s by 16 percent.

Over a decade ago, Congress recognized the importance of high-quality mammography screening by passing the Mammography Quality Standards Act. This act was designed to ensure that mammography is safe and reliable and that breast cancer is detected during its most treatable stages. This act established national standards for mammography facilities, for personnel, including doctors who interpret mammograms, for equipment, and for operating procedures.

This legislation today, H.R. 4555, ensures that American mammography providers continue to be held to high standards and that mammography continues to become a safer, more accurate tool for detecting breast cancer. It makes sense to update and extend this program to make certain we are fighting breast cancer as early as possible and as accurately as possible.

I am pleased to support this important legislation.

Mr. DINGELL. Mr. Speaker, I rise in support of H.R. 4555, the Mammography Quality Standards Reauthorization Act of 2004. I am proud to have introduced this bill, and proud to have helped author the original Mammography Quality Standards Act which has made a major contribution to improving the quality of mammograms.

Just a few months ago, the Institute of Medicine (IOM) published a detailed reported entitled: ''Saving Women's Lives, Strategies for Improving Breast Cancer Detection and Diagnosis.'' According to the IOM, ''[m]ammography is a safety net that saves lives each year, . . . and although mammography saves lives, it is not perfect.'' The IOM report noted that many women who would benefit from mammography do not undergo regular screening and others who do undergo regular screening develop breast cancers that were not detected by their mammography exam. While the report notes that progress has been made in reducing mortality from breast cancer, it is still the second leading cause of death for women.

While research will hopefully lead us to improved techniques for detecting and treating breast cancer, another IOM study entitled: ''Mammography and Beyond: Developing Technologies for Early Detection of Breast Cancer,'' concluded that mammography, while not perfect, is still the best choice for screening the general population to detect breast cancer at early and treatable stages. To be sure, there are important issues regarding quality and access with respect to screening and treatment services, and work on those will continue.

This legislation is almost identical to S. 1879, a bill introduced by Senator MIKULSKI that has already been passed by the Senate. The only substantive difference is the authorization period. Our bill extends the authorization period through FY 2007, two years longer than the Senate bill. But I support a timely completion of various mammography issue studies requested by Senator MIKULSKI, and I look forward to working with her, Chairman BARTON, my other colleagues, and stakeholders, including the Susan G. Komen Foundation, to bring an MQSA reauthorization bill to the President's desk as quickly as possible.

Mr. GREEN of Texas. Mr. Speaker, I rise today in support of the Mammography Quality Standards Act. It is truly fitting for the House to pass a reauthorization of MQSA during October, which is Breast Cancer Awareness Month. This year, more than 215,000 individuals will learn that they have breast cancer. Hopefully, many of these will be early diagnoses, detected by mammograms that have proven time and again to be the most important tool for early detection.

Thanks to the efforts of HHS, the FDA and private advocacy groups, such as the Susan G. Komen Foundation, an estimated 40 million mammograms are performed annually. And thanks to the Mammography Quality Standards Act initially enacted over a decade ago, women all across America have benefited from uniform quality standards for mammography facilities.

For several years, I've been working with the FDA on issues related to silicone breast implants. I am concerned about recent studies on the effect of breast implants on mammography readings.

Specifically, an April 2003 NIH report highlighted clinical studies suggesting that women with breast implants have more advanced cancer at diagnosis than women without breast implants. And more recently, a January 2004 article published in the Journal of the American Medical Association concluded that breast implants decrease the sensitivity of mammography screenings to detect breast cancer.

The FDA has been extremely responsive on this issue and has acknowledged that breast implants can hide tumors or make it more difficult to include them in the image. As such, the FDA has suggested that medical professionals take special implant displacement views in addition to those taken during routine mammograms. These extra views are crucial to ensuring that women with breast implants have effective mammograms.

The folks at FDA have worked wonders on mammography standards thus far. I have every confidence that they will keep up the good work and take into consideration the unique circumstances of women with breast implants. With that, Mr. Speaker, I would encourage all of my colleagues to support this important legislation.

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

The SPEAKER pro tempore. 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. 4555, as amended.

The question was taken; and (two-thirds having voted in favor thereof) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

□ 1500

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. 2929) 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. 2929

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 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 antivirus 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 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.—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 identifying the program, or a statement or other information sufficient to clearly identify the program.

(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 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 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 Commission 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 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 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) 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 11(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 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 information may not include any record of aggregate data that does not identify particular persons, particular computers, particular users of computers, 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 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.

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, 2009.

The SPEAKER pro tempore (Mr. FOSSELLA). 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 and include extraneous material on H.R. 2929.

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 is considering legislation to protect consumers against Internet spying.

Internet spying is all too common. Many consumers are totally unaware that even that their computers can be infected with programs that monitor their activity on the Internet and transfer private information to third parties. At the least, this private information is used to drive the annoying pop-up ads that we see when we turn on our computers. At its very worst, spyware is used by unscrupulous operators to steal financial information and even the individual who owns the computer's personal identity.

The term spyware is used to describe a number of nefarious activities on the Internet, all involve spying or stealing information about consumers without their permission. These activities include: Key stroke logging, in which all of the computer user's key strokes are recorded and sent to a third party; homepage highjacking, in which spyware takes control of the computer, highjacks the individual user's homepage to a commercial or in some case a pornographic site; phishing, in which spyware directs false messages to computer users purporting to be from reputable merchants to steal credit card or other financial information from the user for the use of the third party.

Spyware is downloaded on to a computer without the knowledge of the user. Computers can be infected just by visiting Web sites that cause spyware to be downloaded on to any computer visiting that site.

We tested some of the computers in the Committee on Energy and Commerce. We discovered that these computers had been infected with many pieces of spyware, I believe the number was over 60, and that some of it did direct information to third parties about the use of those computer. All of this was done without any notice to the owners of those computers. I would also point out that this was done by getting through at least two fire walls, the House of Representatives' fire wall and the Committee on Energy and Commerce's fire wall.

Technological development moves quickly, much faster than the regulatory or legislative process. It has taken the House 5 years to give regulators additional tools to combat spam, for instance. I am told that the Federal Trade Commission has not brought any cases against purveyors of spyware to date. Our reaction to spyware is the exception to this rule. In town meetings in my congressional district in Texas just this past August, my constituents unanimously expressed outrage at the brazenness of spyware and exhibited a strong desire for us to act as soon as possible against this insidious disease.

Every Member that I have spoken with on both political parties wants to take action to fight spyware. Some have heard from constituents. One of our subcommittee chairmen experienced the effects of spyware firsthand when his own homepage was highjacked. Today, on a bipartisan basis, it is my hope that we will pass this legislation to combat spyware.

The legislation before us would prohibit the sets of practices like highjacking a consumer's homepage. It

would prohibit keystroke logging. It would prohibit sending ads that cannot be closed except by shutting down the computer. It would also provide for a prominent opt-in for consumers prior to downloading any monitoring software under that consumer's computer.

I believe that consumers should be given notice and have the right to consent before monitoring software that collects information about them is added to their computers.

The legislation before us would also require that monitoring software be easily disabled at the direction of the consumer. It would also provide for FTC, Federal Trade Commission, enforcement with significant monetary penalties for those who knowingly violate the act. While criminal penalties may be appropriate for the most egregious behavior, I believe we have an obligation to provide additional protection to consumers' online information by having these civil fines that the FTC would enforce.

Importantly, the SPY ACT before us regulates information-collection programs. These are programs that have the capability to collect personally identifiable information and either transmit that information to a third party or use that information to deliver or display advertising on the computer. The SPY ACT requires companies that are sending ads to the 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 their own decision as to whether they wish to be so bombarded.

The SPY ACT sets up a uniform national rule. Internet commerce is inherently interstate in nature. We need one set of rules for such commerce. I want to commend a number of Members for their strong work on this bill. First of all, I would like to thank the bill's sponsor, the gentlewoman from California (Mrs. BONO). It is she who has taken the lead to introduce the bill last October when most of us, myself included, had little knowledge of exactly what spyware was. She has been a tireless educator to many of us on its dangers and has worked tirelessly to improve the bill. She has brought dynamic leadership on technology issues to the Committee on Energy and Commerce, and her commonsense approach on this legislation has brought the issue to the floor expeditiously. I want to commend her for her strong work.

The gentleman from New York (Mr. TOWNS), the co-sponsor of the original legislation with the gentlewoman from California (Mrs. BONO), he too has been a great bipartisan partner in this project. He made important contributions to the areas of network- and computer-based security.

The gentleman from Florida (Mr. STEARNS), the chairman of the Subcommittee on Commerce, Trade and Consumer Protection has been a key leader on all privacy related issues in this Congress. He has held eight hearings on privacy matters in this Congress and worked with the gentlewoman from California (Mrs. BONO) and the gentleman from New York (Mr. TOWNS) to perfect the legislation that is before us today.

I would also like to commend the gentleman from Michigan (Mr. DINGELL), the ranking minority member and the gentlewoman from Illinois (Ms. SCHAKOWSKY) the ranking subcommittee member, for their excellent work at the subcommittee and full committee.

We have had truly a bipartisan effort to perfect this legislation and bring it to the floor today. It shows what can happen when Members on both sides of the aisle work together towards a common purpose.

The bill before us is a significant improvement on the original bill. And it is a result of the fine work that has been done by all Members on all sides of the aisle. This is a good bill. It has passed the Committee on Energy and Commerce overwhelmingly.

Anybody who has held a town meeting on this can tell you automatically that our constituents are opposed to spyware and want us to do something to protect their privacy as soon as possible.

Madam Speaker, I hope that we pass this overwhelmingly.

Madam Speaker, I reserve the balance of my time.

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

Madam Speaker, I rise today in support of a strong consumer and privacy protection bill, H.R. 2929, the Securely Protect Yourself Against Cyber Trespass Act or the SPY ACT.

First, I would like to thank my colleagues, the gentleman from Texas (Mr. BARTON), the ranking member, the gentleman from Michigan (Mr. DINGELL), the gentleman from Texas (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 to commend them for the manner in which this bill was handled. The process was open. There was a sincere willingness to address each other's concerns and the work was organized around the goal of creating a strong and effective consumer protection bill. I think we have accomplished our goal.

The SPY ACT is a bill whose time has come. As we have learned from our constituents, friends and family from our own experiences, people are increasingly finding that their home web pages have been changed or that their computers are sluggish. They will get pop-up ads that will not go away no matter how many times they try to close them. They find software on their computer that they did not install and that they cannot un-install. Their computers are no longer their own, and they cannot figure out why. They think that the problem is with their computer, with a faulty program they installed, or with their Internet service provider.

But more and more often, it is becoming clear that they are the unwilling victims of spyware. Software that can collect personal information, track web usage and adversely effect computer performance. While some of the above examples may be written off as merely annoying, there are serious privacy and security issues at stake.

The tracking capability of the software is so powerful that it can record every keystroke a computer user enters. It can snatch personal information from a consumer's hard drive. People can see their bank account numbers, passwords and other personal information stolen because they quite innocently went to a Web site or clicked an agreement which downloaded spyware onto their computer.

Although we do not want to stop legitimate uses of the underlying software, like allowing for access to online newspapers without having to register every time the Web site is visited, we do want consumers to know what is happening with their constitutes and personal information and to stop truly nefarious abuses of the programs, like keystroke logging which can track and transmit every keystroke entered to an unintended recipient.

The SPY ACT ensures that consumers are protected from truly bad acts and actors while also preserving pro-consumer functions of the software. It prohibits indefensible uses of the software, like keystroke logging and homepage highjacking. Additionally, it gives consumers the choice to opt-in to the installation or activation of information-collection programs on their computer, programs that are not spyware, but only when the consumer knows 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 spyware. The SPY ACT puts the control of computers and privacy back in consumers' hands, and I am glad that I was able to be a part of the process that brought this bill to the floor today.

Again, I thank my colleagues for this pro-consumer, pro-privacy and bipartisan piece of legislation.

Madam Speaker, I reserve the balance of my time.

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

Mr. STEARNS. Madam Speaker, I am pleased to support this legislation. I think it provides strong e-commerce protection, not through computer codes but rather through the U.S. legal code, for the American consumer and businesses large and small. And I would like to say at the very onset that we

have support from the industry itself. Microsoft, Time Warner, Dell, Yahoo, eBay, the Business Software Alliance, Humana, EarthLink and several spyware companies themselves.

The SPY ACT of 2004 takes dead aim at unwanted and sometimes malicious programs known as spyware that we all know can link and lurk in cyberspace. They corrupt and compromise computers and their networks and ultimately, Madam Speaker, they cost Americans and the economy major losses in time and money and productivity.

The Federal Trade Commission loosely defines spyware as software ''that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent or that assert control over a computer without the consumer's knowledge.''

The reality is that this deceptive and sometimes fraudulent activity, including the use of spyware, not only has the potential to damage consumer's confidence in e-commerce but also can be used to defraud consumers by stealing their personal financial information, quite literally, from underneath their noses. It is also alarming that estimates now show that these spyware programs have grown in number from about 2 million in August of 2003 to over 14 million today.

The National Cybersecurity Alliance has estimated that over 90 percent of users had some form of adware or spyware on their computers, and frankly, most of them were totally unaware of it. Given the gravity of this threat and its rapid growth, I am proud to say that the Committee on Energy and Commerce, Republicans and Democrats alike, as mentioned by the ranking member, have worked together in a bipartisan fashion. Oftentimes, we are on the House floor, we will be here probably the next couple of days, not in a bipartisan fashion, but we are here today, and it is a credit to the leadership for bringing this bill before us.

Obviously, I think great credit goes to my colleague, the gentlewoman from California (Mrs. BONO) for her early leadership in this area and also working in a bipartisan method. I think a lot of credit goes to the gentleman from New York (Mr. TOWNS) for his early co-sponsorship. And I think our Subcommittee on Commerce, Trade and Consumer Protection, which I chair, and the gentlewoman from Illinois (Ms. SCHAKOWSKY) is the ranking member, also as she pointed out, worked together.

I would also like to tell my colleagues, this is another good effort of our staffs, both Democrat and Republican, working together. The hard work of industry also should be commended because, obviously, when this bill first got started and we had our hearings, there were a lot of people in the industry that had some reservations.

□ 1515

We can only get through those reservations by having open-door communications with them and making the case of hard work with the staff and trying to get this free flow of communication, and I think in this case the staff is to be commended for making, as the chairman said, a good bill even better.

As I mentioned to him, I have had many hearings dealing with privacy, and we have had a hearing on this. So H.R. 2929 would not only send a loud and clear message to those who would do harm to our computers but it also would add another layer of protection over the robust firewall and detection technology that the information technology industry is starting to provide consumers and businesses.

In conclusion, Madam Speaker, I urge my colleagues to pass H.R. 2929, the SPY Act of 2000. It is time to put an end to spyware and keep Americans secure and confident in the e-commerce marketplace.

Ms. SCHAKOWSKY. Madam Speaker, I would like to join the gentleman in thanking our staff, as well, for the hard work and the good work they did on bringing this legislation now to fruition.

Madam Speaker, I yield 5 minutes to the gentleman from New York (Mr. TOWNS), one of the people most responsible for this consumer protection legislation.

Mr. TOWNS. Madam Speaker, I rise in support of the SPY Act, which would greatly improve the privacy of consumers' online computer use.

A lot of hard work has been put into this legislation. First and foremost, I would like to commend the gentlewoman from California (Mrs. BONO), the primary sponsor of the bill. Without her hard work, insight and persistence on this issue, we would not be here today. As the primary Democratic sponsor, I have been proud to work with her on this bill, and I salute her for all her efforts.

I also want to commend the gentleman from Texas (Chairman BARTON) for his strong commitment to this issue and leadership in getting our bill to the floor. I would like to thank the gentleman from Florida (Chairman STEARNS), the gentleman from Michigan (Ranking Member DINGELL), and the gentlewoman from Illinois (Ranking Member SCHAKOWSKY), who have all made substantial contributions. I would also like to acknowledge all of the staff that have worked so hard to make this day a reality.

There is no debate that spyware is a serious problem, one that is growing and becoming more harmful every day. Spyware software, which is downloaded without the computer owner's knowledge, invades our privacy by recording and transmitting personal information, monitoring the Web sites we visit, or even stealing documents from our computers. Other programs hijack our computers by changing our home page or forcing us to click through multiple screens until we download a spyware program.

Today's legislation would give consumers new tools to prevent these harmful activities from happening. Under the bill, consumers would have to receive a clear and concise warning about the spyware program. Second, consumers would have to provide their affirmative consent before the program could operate on their computer. Finally, consumers must have the option to easily disable any harmful spyware program on their computer.

While some consumers may want to share their information to receive free games or other discount offers, all consumers have the right to make that choice. This legislation would help ensure that consumers who do not want these programs secretly operating in the background, recording personal information, are not on their computers.

Finally, Madam Speaker, any time we legislate on highly technical matters, there is always a danger in stifling innovation or making the use of legitimate software too burdensome. It is a very difficult tightrope to walk, but I think we have done an excellent job in walking that line. This bill addresses many of the concerns raised, while at the same time retaining meaningful notice and consent to protect consumers' privacy.

This is a classic example of what we can accomplish when we work together, and we have worked together to make this day a reality. Through much hard work, we have carefully crafted a strong, bipartisan consumer protection bill; and I urge my colleagues to support this legislation because it is needed and needed desperately.

Mr. BARTON of Texas. Madam Speaker, I want to thank the gentleman from New York who just spoke for his excellent leadership on this bill. It is a better bill because of his efforts.

Madam Speaker, I yield 5 minutes to the distinguished gentlewoman from California (Mrs. BONO), who, along with the gentleman from New York (Mr. TOWNS), was an original cosponsor of the original bill.

Mrs. BONO. Madam Speaker, first I would like to thank the gentleman from Texas for yielding me time and for his tremendous leadership on this issue, as well as all of the issues before the Committee on Energy and Commerce.

I would also like to extend my gratitude to the gentleman from Michigan (Ranking Member DINGELL), the gentleman from Florida (Chairman STEARNS), a good friend, the gentlewoman from Illinois (Ranking Member SCHAKOWSKY) and the original cosponsor along with me, the gentleman from New York (Mr. TOWNS), who has been an absolute pleasure and delight to work with. I look forward to working with him on a lot more similar issues in the future.

Each of the aforementioned colleagues of mine, as well as their staffs,

have worked with me to improve and refine this bill. I also thank the industry participants and consumer groups who have contributed to its improvement. I am confident that we have drafted a bill that protects consumers without impeding the growth of technology.

I would also like to thank all my staff and Jennifer Baird and Linda Valter for their tireless work.

In the other body, Senators BURNS, WYDEN, AND BOXER introduced S. 2145, the SPY BLOCK Act, and the Senate Commerce Committee recently approved and reported the bill. I look forward to working with my Senate counterparts on this matter, as well as the FTC and the technology industry, which will hopefully work to educate consumers about the dangers surrounding spyware, as well as its nature.

In California, my home State, Governor Schwarzenegger, recently signed an anti-spyware bill entitled the Consumer Protection Against Computer Spyware Act. This bill, similar to other State laws, varies from the proposed Federal legislation, making it all the more imperative that we act now to ensure there is a uniform standard available for consumers.

Yesterday, Earthlink and Webroot just released their latest spyware audit, which reveals that after 3 million scans for spyware, 83.4 million instances of spyware had been discovered. This is an average of 26 traces of spyware per SpyAudit scan. Unfortunately, consumers regularly and unknowingly download software programs that have the ability to track their every move. Consumers are sometimes informed when they download such software. However, the notice is often buried in multithousand word documents that are filled with technical terms and legalese that would confuse even a high-tech expert. Moreover, there are some Web sites and e-mail messages which deliberately trick computer users.

In response to the rapid proliferation of spyware, in July of 2003, together with the gentleman from New York (Mr. TOWNS), I introduced H.R. 2929, the Securely Protect Yourself Against Cyber Trespass Act. This bill prohibits such behavior by specifically outlawing Web hijacking, keystroke logging, drive-by downloads, phishing, and several other insidious behaviors.

Additionally, H.R. 2929 establishes a simple notice regime so the computer users can make informed decisions regarding programs they wish to put on their computers. The PC has become our new town square and global market, as well as our private database. If a consumer downloads software that can monitor the information shared during transactions, for the sake of the consumer as well as e-commerce, it is imperative that the consumer be informed of whom he or she is inviting into their computer and what he or she is capable of doing. After being informed, a consumer should have the chance to decide whether to continue with that download.

H.R. 2929 would require that all spyware companies give clear, concise and conspicuous notice to computer users about the function of their software, as well as the information that may be collected and transmitted through such software. After giving such notice, the computer user would have to agree to further download that software.

Madam Speaker, I urge my colleagues to support H.R. 2929. Again, I thank the chairman and my colleagues on the other side of the aisle.

Ms. SCHAKOWSKY. Madam Speaker, if I could inquire if there are any other speakers on the other side.

Mr. BARTON of Texas. We think we have the gentleman from Michigan (Mr. UPTON), subcommittee chairman, on his way; but other than that we have no other speakers.

Ms. SCHAKOWSKY. Madam Speaker, I have no other speakers, and I yield back the balance of my time.

Mr. BARTON of Texas. Madam Speaker, I yield myself the balance of the time.

To close the debate, let me simply say I think we have seen in this debate not just the bipartisan support but the unanimous support this bill has. Whether my colleagues represent metropolitan New York City or the suburbs of Chicago or the hurricane-ravaged plains of Florida, the prairies of Texas, or Southern California, we are all hooked up to the Internet; and we all have constituents who are outraged that as they do their Internet shopping and browsing and surfing, these insidious programs called spyware can infect their computers without their permission. Unfortunately, right now it is not even illegal.

What this bill does is make it illegal, and it gives the Federal Trade Commission the authority to impose significant civil fines for using this spyware.

I would also like to point out that thanks to the strong work of the committee staff on both sides of the aisle, we have a bill that the business community supports. Microsoft, the Software Business Alliance, Yahoo, Time Warner who owns AOL, they all support this. Ebay supports this bill. We are going to put those statements of support in the RECORD at this point.

TIMEWARNER,
September 21, 2004.

Hon. JOE BARTON,
Hon. JOHN DINGELL,
House Energy and Commerce Committee, House of Representatives, Rayburn House Office Building, Washington, DC.

DEAR CHAIRMAN BARTON AND REPRESENTATIVE DINGELL: On behalf of TimeWarner and its AOL division, I would like to express our support for H.R. 2929, the Safeguard Against Privacy Invasions Act, which was authored by Representatives Bono and Towns and approved by your Committee in June.

Battling spyware is one of AOL's top business and policy priorities. Spyware is a growing concern for all Internet users, wreaking havoc with consumers' computers and undermining their online experience. We believe that spyware must be addressed on many fronts, including through legislation, technology, and consumer education.

We have been pleased to work closely with the House Energy and Commerce Committee over the past several months on this legislation. H.R. 2929 will provide some important tools in the fight against spyware, outlawing destructive behaviors that can deceive and defraud consumers through the use of unauthorized software. We appreciate all of the improvements you have made and continue to make to this bill as it moves through the process, and we are hopeful that, along with legislation that has been approved by the Judiciary Committee, it will soon be considered on the House Floor.

The time is right for strong and effective federal spyware legislation. We are grateful for the opportunity to work with you and your Committee on this topic, and are eager to see this bill move forward so that consumers and legitimate businesses can enjoy additional anti-spyware protections in the near future.

Sincerely,

JENNIFER JACOBSEN,
Vice President, Global Public Policy.

BUSINESS SOFTWARE ALLIANCE,
Washington, DC, September 17, 2004.

Hon. JOE BARTON,
Chairman, House Energy and Commerce Committee, Rayburn House Office Building, Washington, DC.

DEAR MR. CHAIRMAN: Thank you for your ongoing efforts to advance America's high tech industries and protect the interests of American consumers. We appreciate your commitment and leadership.

In particular, I write today to commend you for your attention to addressing the growing problem of spyware and to let you know that the Business Software Alliance endorses your leadership in moving to secure approval of the Spy Act, H.R. 2929, on the House floor this Congress. The manager's amendment to the committee passed bill, which we understand will be brought to the floor, is a step forward in the effort to control the onslaught of harmful spyware that has proved to be annoying at best and harmful at its worst to consumers and businesses alike.

Surreptitiously downloaded spyware inflicts significant costs on our member companies as they are forced to help their innocent customers identify and remedy the source of parasitic encroachment on their computer systems. As an association that represents the country's leading business software and hardware makers, we know all too well the dangers of harmful and deceptive spyware. We have heard from our customers, just as you have from your constituents, that this spyware is frustrating the user experience by hijacking their personal property.

I also want to commend you and your staff on the development of the legislation. As you know, the initial drafts raised concerns that the bill might target and punish technologies rather than the bad behavior that has proved to be so troublesome. I am pleased that you and your staff provided an open and inclusive environment for us to share our views and appreciate the improvements that have been made to the legislation.

As you know, successful legislation requires thoughtful discussion, cooperation and compromise, and we understand the important balance you have sought to achieve in moving this process forward. We applaud

your efforts, and BSA looks forward to working with you and your staff as the bill continues through the legislative process.

Sincerely,

ROBERT W. HOLLEYMAN, II,
President and CEO.

SEPTEMBER 21, 2004.

Hon. JOE BARTON,
Chairman, House Committee on Energy & Commerce, Rayburn House Office Building, Washington, DC.
Hon. JOHN DINGELL,
Ranking Member, House Committee on Energy & Commerce, Rayburn House Office Building, Washington, DC.

DEAR CHAIRMAN BARTON AND CONGRESSMAN DINGELL: On behalf of eBay and its more than 100 million users worldwide, I want to commend you for your bipartisan work on legislation intended to combat Spyware on the Internet.

We agree that the proliferation of so-called ''Spyware'' on the Internet threatens to undermined consumers' online experience and erode the overall value of the Internet. eBay is always ready to work with lawmakers to come up with sound legislation that prohibits invasions of privacy while protecting legitimate activities we use to protect our community and fight fraud. We believe the Energy & Commerce Committee has worked hard to strike the necessary balance on this important issue, and has gone to unprecedented lengths to reach bipartisan consensus and work with industry leaders.

One of eBay's highest priorities is to provide a safe and well-lit place for our users to conduct business. That is why we are pleased with the Committee's willingness to include a provision exempting fraud detection and prevention activities from the bill's requirements intended to deter Spyware. That provision will allow us to continue to gather critical information needed to protect our users when they trade on eBay.

Thank you for taking eBay's concerns into consideration in developing balanced legislation to target nefarious behavior on the Internet. We look forward to full House consideration of this important legislation as soon as possible.

Sincerely,

TOD H. COHEN,
Associate General, Global Government Relations.

HUMANA INC.,
Louisville, KY, September 15, 2004.

Re H.R. 2929—the Safeguard Against Privacy Invasions Act.

Hon. JOE BARTON,
Chairman, House Energy and Commerce Committee, Washington, DC.

DEAR CHAIRMAN BARTON: I wish to express my company's strong support for the Committee-reported version of H.R. 2929, the Safeguard Against Privacy Invasions Act, or SPY Act. This legislation provides a meaningful opportunity to reduce the amount of spyware and disruptive advertising that are threatening to impair our day-to-day business applications. Moreover, such reduction will enhance the protection of our customers' personal information and improve their online experience.

Humana Inc., headquartered in Louisville, Kentucky, is one of the nation's largest publicly traded health benefits companies, with approximately 7 million medical members located primarily in 19 states and Puerto Rico. We offer coordinated health insurance coverage and related services—through traditional and internet-based plans—to employer groups, government-sponsored plans and individuals. We have approximately 13,000 employees.

At Humana, we have experienced significant spyware-related damage on our workstations. This includes computer-related printing problems, inability to operate internal applications like entering timesheets and expense reports, serious performance degradation (slow response time), and the inability to launch or use the Internet or our internal intranet applications. We have numerous workstations that have needed to be rebuilt because of spyware issues and service calls where our technicians spend numerous hours troubleshooting various spyware problems. We estimate that we received approximately 300,000 individual pieces of malicious spyware in the first quarter of 2004 alone (or approximately 5 percent of all transactions.)

Not every associate or consumer has the sophistication level of knowing what is or may not be installed on his or her PC—causing spyware-related response time issues. As a result, we believe that surreptitiously installed spyware introduces very serious privacy concerns both at an individual level and for corporations. Unknowingly being spied upon seems to also introduce new types of concerns for corporations, including protection of intellectual assets, property, trade secrets, and competitive advantage information.

Additionally, as a company whose core business is to handle our customers' most sensitive medical information, we strongly support the concept that consumers need to be meaningfully informed about how their personal information is collected and used. And, we support their right to end that relationship when they deem fit to do so. There is no such thing as ''benign'' spyware.

The health care industry continues to be one of the most paper-intensive industries. In the past several years, we have made great strides to move toward an electronic world. E-commerce and the Internet in the health care industry have reduced administrative costs, improved claims processing, and hold the promise of improving patient care and quality through concepts such as electronic medical records. The proliferation of spyware and disruptive software threatens to undermine consumers' confidence in the Internet and negate the progress we have made and hope to make in the future. Therefore we fully support moving forward with this important legislation.

In closing, we appreciate the opportunity to comment on H.R. 2929, and look forward to assisting the Committee in any way as this legislation moves forward.

Sincerely,

BRUCE J. GOODMAN,
Senior Vice President and Chief Service and Information Officer.

MICROSOFT CORPORATION,
Washington, DC, September 22, 2004.

Hon. JOE BARTON,
Chairman, House Energy and Commerce Committee, House of Representatives, Washington, DC.
Hon. JOHN D. DINGELL,
Ranking Member, House Energy and Commerce Committee, House of Representatives, Washington, DC.

DEAR CHAIRMAN BARTON AND RANKING MEMBER DINGELL: I am writing to commend your leadership on H.R. 2929, the ''Securely Protect Yourself Against Cyber Trespass Act'' or the ''SPY ACT,'' and convey Microsoft's support for moving the bill forward for consideration by the full House.

Microsoft shares the goals of the members of the Energy and Commerce Committee to protect consumers from deceptive software (''spyware''). We agree: the fraudsters that use deceptive software to prey on consumers must be stopped. We appreciate your and your staff's tireless work toward producing a bill that, as you put it, goes after the bad guys but doesn't unnecessarily impede the good guys.

Legislation is but one tool with which to wage the fight against spyware. In addition to strong laws, Microsoft strongly believes that technological solutions, consumer awareness, best practices, and strong enforcement are all critical elements of any effective strategy to help unsuspecting consumers avoid being victimized by spyware.

In particular, I want to express our appreciation for working to address concerns with Section 3 of H.R. 2929 which imposes notice and consent requirements to protect the privacy of computer users. We appreciate the work of the staff to understand potential consequences of such requirements in instances where exchange of data is related to the functionality of particular software applications or where it would be reasonably expected by computer users.

Finally, let me personally convey Microsoft's appreciation for the opportunity to provide input to you and the committee staff throughout this process. We would not have reached this point without their diligence and serious consideration of our feedback.

Like any legislation of such complexity, there may be additional areas that need to be clarified or enhanced. With that in mind, we look forward to continuing to work in partnership with you and the bipartisan committee staff should such issues arise. Likewise, please do not hesitate to call on us should you require our input or assistance.

Thank you for the enormous amount of time and effort you have devoted to this important effort.

Sincerely,

JACK KRUMHOLTZ,
Managing Director, Federal Gov. Affairs, Associate General Counsel.

YAHOO! INC.,
SEPTEMBER 17, 2004.

Hon. JOE BARTON,
Energy & Commerce Committee,
2322 Rayburn House Office Building, Washington, DC.

DEAR MR. CHAIRMAN, Yahoo! writes to support the latest version of H.R. 2929 issued on September 10, 2004, and looks forward to continuing to work with you as the bill proceeds through the legislative process.

You, Ranking Minority Member Dingell, Subcommittee Chairman Stearns, Ranking Member Schakowsky, and co-authors of the bill Representatives Bono and Towns and the respective staff, have worked tirelessly to develop a bill that prohibits ''spyware'' activities such as taking control of a user's computer or modifying computer settings for the purposes of causing damage. In addition, the bill gives users more control over their online experience through enhanced notices and features that can disable aspects software consumers may find undesirable. The new requirements strike a balance between allowing useful tools for computer users and requiring reasonable changes to existing mechanisms to give notice, consent, and to remove or disable software.

Thank you for hearing our concerns, responding to them accordingly, and giving consumers and legitimate businesses hope that the spyware problem can be, in part, addressed by new tools for consumers and the new deterrent penalties in H.R. 2929.

Sincerely,

JOHN SCHEIBEL,
Vice President for Public Policy.

UNITED STATES TELECOM ASSOCIATION,
Washington, DC, August 4, 2004.

Hon. DENNIS HASTERT,
House of Representatives,
Washington, DC.

DEAR MR. SPEAKER: On behalf of the United States Telecom Association (''USTA''), I am writing to express our support of H.R. 2929, the Safeguard Against Privacy Invasions Act. USTA was grateful for the opportunity afforded by members of the House Commerce Committee specifically Chairman Barton, Representatives Stearns, Upton, Bono, Dingell Towns, and Schakowsky and their staff to participate and comment on this legislation. USTA represents over 1,200 member companies that offer a wide range of services, including local exchange, long distance, wireless, Internet and cable television service.

H.R. 2929 recognizes appropriately the role of telecommunications carriers as it relates to network integrity, security and the transmission of information. In late June, the House Commerce Committee voted 45–4 to send this legislation to the full House and it is our hope that it will be considered in the coming weeks.

Again, thank you for all you do on behalf of the telecommunications industry. Please do not hesitate to contact me if I may be of service to you or your staff.

Sincerely,

WALTER B. MCCORMICK, JR.
President and Chief Executive Officer.

WHENU,
New York, NY, September 20, 2004.

Re H.R. 2929.

Hon. JOE BARTON,
Chairman, Committee on Energy and Commerce,
House of Representatives, Washington, DC.

DEAR CHAIRMAN BARTON: WhenU.com is a global Desktop Advertising Network. Through the Company's partnerships with popular software developers, WhenU enables consumers to receive valuable software for free by agreeing to see occasional ads instead of paying a fee—and without compromising their privacy. WhenUs's unique advertising technology distinguishes itself from existing online advertising approaches by applying sophisticated precision logic at the desktop level. From the desktop, WhenU software examines keywords, URLs and search terms currently in use on the consumer's browser and then selects relevant and useful advertisements. WhenU accomplishes this in a highly privacy protective manner and avoids collecting any browsing data—even anonymously—about individual users. The WhenU Desktop Advertising Network does not track user or clickstream data, use cookies, compile a centralized database of users, or engage in any type of user profiling.

I am writing to first express my appreciation to you, Chairman Stearns, and Representatives Bono, Schakowsky and Towns, among others, and to the bipartisan Energy and Commerce Committee staff led by David Cavicke, for the opportunity to work with the Committee to help perfect H.R. 2929. It has been a gratifying, productive and successful process. I am pleased today to state that WhenU supports the September 10 version of H.R. 2929. We are particularly pleased with the bill's treatment of state pre-emption issues. We believe that the September 10 version of H.R. 2929 strikes a reasonable balance that should succeed in protecting consumers, eliminate bad actors, and enable legitimate businesses to continue to provide useful and meaningful e-commerce solutions for the country.

Sincerely,

AVI NAIDER,
Chief Executive Officer.

180SOLUTIONS,
Bellevue, WA, September 17, 2004.

Hon. JOE BARTON,
Chairman, Committee on Energy and Commerce,
Rayburn House Office Building, House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN. 180solutions is a leading provider of Internet search marketing software, offering consumers access to a wide range of free content in return for their agreement to be shown a limited number of websites each day selling goods or services—most often at times when they are likely shopping for those goods or services online. We use keyword search technology to deliver these highly targeted websites to consumers on behalf of over 6,000 advertisers, including many top-tier companies whose brands are household names.

We are writing to express our company's support for House passage of H.R. 2929 in the form of the Managers' Amendment dated September 10, 2004. During the course of this legislation's consideration in the Energy and Commerce Committee, it has continually evolved and improved to allow legitimate companies like ours to assist consumers in their search for advantageous and competitive sales offers online, while protecting computer users and owners from the deceptive or fraudulent acts or practices often associated with spyware. We are also deeply appreciative of the open process by which the bill has been developed and commend the Members and staff on both sides of the aisle for working with all stakeholders to that end.

As you may know, we had hoped the legislation would deal more with tracking cookies, but we recognize that the issue is complex and thus has become controversial. The Federal Trade Commission report provided for by section 8 of the Managers' Amendment is a good compromise that will foster further discussion on the basis of sound and unbiased analysis.

Thank you again for your consideration of our views and for your careful crafting of this legislation.

Sincerely,

KEITH SMITH,
Chief Executive Officer.

This is one of those rare times when the House of Representatives probably is not ahead of the curve, but we are at least catching up with the curve to end something and to police something that every one of our constituents who is on the Internet is absolutely opposed to.

So Madam Speaker, I ask for a strong ''aye'' vote on this bill.

Mr. SHAYS. Madam Speaker, I want to express support for two bills the House is considering this week: H.R. 2929, the Safeguard Against Privacy Invasions Act, and H.R. 4661, the Internet Spyware I–SPY Prevention Act. I strongly support these pieces of legislation and I am pleased they incorporate changes similar to legislation Congressman JAY INSLEE and I introduced, H.R. 4255, the Computer Software Privacy and Control Act.

Millions of computers have been infected with spyware, software that is deceptively installed on their computers to collect their personal information, record their keystrokes, change their browser homepage, or display unwanted advertising.

H.R. 2929 would require notice and consent from the computer user before software is able to collect personal information and transmits it to a third party, monitor Internet usage, such as websites visited, modify computer settings or deliver advertisements. This provision accomplishes a main goal of the Computer Software Privacy and Control Act.

H.R. 4661 strengthens criminal provisions in the Computer Fraud and Abuse Act. Providing necessary criminal penalties for spyware will help prevent this deceptive activity and protect the privacy of consumers. Our legislation includes provisions similar to this as well.

I am glad H.R. 2929 and H.R. 4661 require notice and consent and strengthen criminal provisions, and I urge my colleagues to support these important pieces of legislation.

Mr. GOODLATTE. Madam Speaker, I rise today to discuss H.R. 2929, the ''Safeguard Against Privacy Invasions Act.''

I believe that there is a need to impose appropriate civil penalties against those who use software to commit egregious acts against computer users. In that respect, the provisions in H.R. 2929 that impose civil penalties on the truly bad actors, including those who use spyware to take over a user's computer to send spam, or those who engage in keystroke logging to steal personal information, are a step in the right direction.

However, I also have concerns that portions of the bill cast too wide a net and that they would have unintended consequences that could penalize the legitimize software companies that are actually trying to play by the rules. Many provisions of this bill would not only encompass spyware, but also legitimate interactive software services. I oppose the provisions of this bill that stretch beyond punishing the truly bad actors and instead create a static regulatory regime in an industry that is always innovating and changing to respond to consumer demand.

Also, imposing a notice and consent requirement for most software that is loaded onto computers could create unintended consequences. Specifically, when consumers are faced with the multiple notices that would be required under this bill, they will likely become desensitized and stop reading the disclosure altogether. The result could be a heavy-handed regulation that does not even achieve the desired goals of informing consumers and protecting them from spyware, especially since the truly bad actors are likely to simply ignore these regulations.

I have introduced legislation, H.R. 4661, the Internet Spyware I-SPY Prevention Act, which impose tough criminal penalties on the most egregious purveyors of spyware without imposing a broad regulatory regime on legitimate software providers. I believe that this more targeted approach is the best way to combat spyware.

While I have serious reservations about many portions of H.R. 2929, I also believe that it contains many civil prohibitions that would help in the fight against spyware. I support this bill, not in its entirety, but as an acknowledgement that some civil penalties are appropriate in the fight against spyware when properly targeted. However, I remain concerned about the broad regulatory aspects of this legislation, and hope to continue working to ensure that the final legislation is appropriately targeted at the truly bad actors, and that it does not cast a broad regulatory burden on those who continue to innovate and create new and exciting services in the interactive software industry.

Ms. JACKSON-LEE of Texas. Madam Speaker, I join my colleagues today to support H.R. 2929. Persistent computer security vulnerabilities may expose U.S. critical infrastructure and government computer systems

to possible cyber attack by terrorists, possibly affecting the economy or other areas of national security. Because of the ubiquitous nature of the Internet, unprotected home computers—often lacking network security features, could be the entree for cyber attacks. Even when national security is not at issue, spyware programs could be used to harvest personal informaiton—such as bank or credit card account number and e-mail addresses—from computers. This information could be used subsequently in fraudulent criminal activities or in the sending of unauthorized SPAM e-mail messages.

Unwanted spyware programs can make changes to a computer that can be annoying and can cause the computer to slow down or crash. These programs have the ability to change the home page of a computer user's Web browser or search page, or add additional components to the browser that are unnecessary or unwanted. These programs could make it very difficult to change the settings back to the way they were originally.

This bill directs the Federal Trade Commission (FTC) to prohibit the transmission of an unauthorized spyware program to a covered computer over the Internet. The bill further establishes requirements for an affirmative agreement by the user of the covered computer to specifically agree the conditions of the transmission with an acknowledgement of the person and address of the transmitter.

The bill provides specific prohibitions on use of any spyware program for collecting any personally identifiable information from the covered computer unless notice is provided. The criminal penalties provided for in this act will help to provide a necessary enforcement mechanism.

I believe this is just one of the steps necessary to secure the nation's critical infrastructure and to help protect the privacy and civil liberties of Americans.

Mr. DINGELL. Madam Speaker, ''Barbarians At the Digital Gate'' recently warned the front page of the Sunday New York Times Business Section. What elicited this alarming headline? Pernicious computer software commonly called ''spyware'' and ''adware''.

These programs sneak onto 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 has brought Internet use to a crossroads. It threatens legitimate Internet commerce. Consumer complaints are deluging computer call centers and regulators. The most common complaints are: hijacked home pages, redirected Web searches, a flood of pop-up ads, and sluggish and crashed computers.

The bill, as amended, prohibits a number of deceptive acts or practices related to spyware, and provides for 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, diagnostics and repair, and fraud detection from the SPY Act. It is a carefully balanced bill.

Most importantly, this legislation contains opt-in protection for consumers. It 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.

I also note that 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.

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., Humana Inc., Microsoft, 180 Solutions, Time Warner/AOL United States Telecom Association, WhenU, and Yahoo!—all of whom have submitted letters of support.

The bill has improved at every stage of its consideration, and I want to commend the leadership and hard work of Rep. BARTON, the Chairman of the Committee on Energy and Commerce, Reps. STEARNS and SCHAKOWSKY, the Chairman and Ranking Member, respectively, of the Commerce, Trade, and Consumer Protection Subcommittee, and Reps. BONO and TOWNS, the lead Republican and Democrat sponsors of the bill. I also commend the bipartisan staff team who worked very hard over the last five months to get this bill to the Floor this year; David Cavicke, Shannon Jacquot, Crhis Leahy, Brian McCullough, Will Carty, Jennifer Baird, Consuela Washington, Diane Beedle, and Andrew Delia.

I urge my Colleagues to vote ''yes'' on passage of H.R. 2929. It is a good bill. It's good for consumers. And it is good for honest commerce on the Internet.

Mr. GREEN of Texas. Madam Speaker, my interest in the consumer problem of spyware stems from many years of work on the consumer spam problem.

The anti-spam law was not expected to eliminate unwanted email, but it did draw a line for consumers—that some kinds of privacy invasion are not allowed. Internet Service Providers like Microsoft, AOL, Yahoo, and Earthlink along with State Attorney Generals are bringing serious actions against spammers who violate the law.

Spyware and illegal spam are not just problems of privacy and convenience, both can be the cause of viruses and other computer crimes.

Just like robbery and speeding have not been eliminated, neither will spam or spyware. But when something is harming social welfare and consumers are overwhelmed, and private sector solutions are not enough, then we need an enforceable standard.

This legislation prohibits the most commonly known deceptive acts and practices related to Spyware from tracking your web surfing habits to send you advertising to hijacking your passwords and credit care numbers.

However, while some use this technology to deceive and defraud us, this technology is also used to support our efforts in national security. This important use of technology is taken into consideration by this bill and exempts law enforcement, national security agencies, network security programs and diagnostics on repairs to our computers from the SPY Act.

In addition, state attorney generals will have the ability to enforce consumer protection laws against spyware and preserves state trespass, contract tort and fraud laws.

This legislation will draw a line that spying on Americans' computers will not be tolerated. Will some people continue to get away with it? Perhaps. But will some people be prosecuted and punished for violating our privacy? Absolutely.

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

The SPEAKER pro tempore (Mrs. MILLER of Michigan). 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. 2929.

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. Madam 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.

RECOGNIZING COMMUNITY ORGANIZATION OF PUBLIC ACCESS DEFIBRILLATION PROGRAMS

Mr. BARTON of Texas. Madam Speaker, I move to suspend the rules and agree to the concurrent resolution (H. Con. Res. 250) recognizing community organization of public access defibrillation programs.

The Clerk read as follows:

H. CON. RES. 250

Whereas coronary heart disease is the single leading cause of death in the United States;

Whereas every two minutes, an individual suffers from cardiac arrest in the United States, and 250,000 Americans die each year from cardiac arrest out of hospital;

Whereas the chance of survival for a victim of cardiac arrest diminishes by ten percent each minute following sudden cardiac arrest;

Whereas 80 percent of cardiac arrests are caused by ventricular fibrillation, for which defibrillation is the only effective treatment;

Whereas 60 percent of all cardiac arrests occur outside the hospital, and the average national survival rate for an out-of-hospital victim of cardiac arrest is only five percent;

Whereas automated external defibrillators (AEDs) make it possible for trained non-medical rescuers to deliver potentially life-saving defibrillation to victims of cardiac arrest;

Whereas public access defibrillation (PAD) programs train non-medical individuals to use AEDs;

Whereas communities that have established and implemented PAD programs that make use of AEDs have achieved average survival rates as high as 50 percent for those individuals who have suffered an out-of-hospital cardiac arrest;

Whereas successful PAD programs ensure that cardiac arrest victims have access to