

SECURELY PROTECT YOURSELF AGAINST CYBER
TRESPASS ACT

JULY 20, 2004.—Committed to the Committee of the Whole House on the State of
the Union and ordered to be printed

Mr. BARTON of Texas, from the Committee on Energy and
Commerce, submitted the following

R E P O R T

[To accompany H.R. 2929]

[Including cost estimate of the Congressional Budget Office]

The Committee on Energy and Commerce, to whom was referred 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, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

	Page
Amendment	2
Purpose and Summary	7
Background and Need for Legislation	7
Hearings	9
Committee Consideration	9
Committee Votes	9
Committee Oversight Findings	11
Statement of General Performance Goals and Objectives	11
New Budget Authority, Entitlement Authority, and Tax Expenditures	11
Committee Cost Estimate	11
Congressional Budget Office Estimate	11
Federal Mandates Statement	13
Advisory Committee Statement	13
Constitutional Authority Statement	13
Applicability to Legislative Branch	13
Section-by-Section Analysis of the Legislation	13
Changes in Existing Law Made by the Bill, as Reported	18
Exchange of Committee Correspondence	18

AMENDMENT

The amendment is as follows:

Strike all after the enacting clause and insert the following:

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 in connection with 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, 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;

(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.

(3) Collecting personally identifiable information through the use of a key-stroke logging function or similar 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 information to another person by misrepresenting the identity or authority of the person seeking the information.

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

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

(b) **EFFECTIVE DATE.**—This section shall take effect 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, or

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

unless, before the first 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 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 in a form and manner 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 substantially similar language:

(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 to grant or deny consent referred to in subsection (a) by selecting an option to grant or deny 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 grants or denies consent using the option required under subparagraph (C) (or selects the option required under subparagraph (D)).

(2) **SINGLE NOTICE.**—The Commission shall provide that, in the case in which multiple information collection programs first execute any of the information collection functions of the programs together, notice in accordance with paragraph (1) may be provided through 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) with respect to each such information collection program.

(3) CHANGE IN INFORMATION COLLECTED.—After an owner or authorized user has granted consent to execution of an information collection program pursuant to a notice in accordance with this subsection, 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 any type or for any 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 first 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.

The Commission may issue regulations to carry out this paragraph.

(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 is accompanied by a statement that clearly identifies the information collection program.

(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), except that the maximum civil penalty for a violation of this Act shall be one of the following amounts, as the Commission, in its discretion, seeks for such a violation:

(1) TREATMENT OF CONDUCT AFFECTING MULTIPLE COMPUTERS AS SEPARATE VIOLATIONS.—\$33,000 for each violation of section 2, and \$11,000 for each violation of section 3, except that in applying this paragraph each separate protected computer with respect to which a violation of such section occurs as a result of a single action or conduct that violates section 2 or 3 shall be treated as a separate violation.

(2) TREATMENT OF CONDUCT AFFECTING MULTIPLE COMPUTERS AS A SINGLE VIOLATION.—\$3,000,000 for each violation of section 2, and \$1,000,000 for each violation of section 3, except that in applying this paragraph—

(A) any single action or conduct that violates such section 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.

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

(c) 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 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 NETWORK SECURITY.**—Nothing in this Act shall apply to any monitoring of, or interaction with, a subscriber’s Internet or other network connection or service by a telecommunications carrier, cable operator, or provider of information service or interactive computer service for network security purposes, diagnostics or repair in connection with a network or service, or detection or prevention of fraudulent activities in connection with a service or user agreement.

(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.

SEC. 6. EFFECT ON OTHER LAWS.

(a) **PREEMPTION OF STATE LAW.**—

(1) **PREEMPTION.**—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 context-based triggering mechanisms or similar means to display an advertisement that partially or wholly covers or obscures content on a Web page in a way that interferes with the ability of the user of a computer to view the Web page.

(2) **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 10(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. REGULATIONS.

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.

SEC. 9. 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” means, with respect to information and for purposes only of section 3, to obtain in a manner other than by transfer by an

owner or authorized user of a protected computer to the party intended as recipient of the transferred information.

(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 a cookie or other text file, data, or computer software, 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 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) An account number.
- (viii) Any access code or password, other than an access code or password transmitted by an owner or authorized user of a protected computer to register for, or log onto, a Web page or other Internet service that is protected by an access code or password.
- (ix) Date of birth, birth certificate number, or place of birth of an individual, except in the case of a date of birth required by law to be transmitted or collected.

(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 com-

puters, or particular email addresses or other locations of computers with respect to the Internet.

(14) 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).

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

(16) 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. 10. 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.

PURPOSE AND SUMMARY

H.R. 2929, the “Securely Protect Yourself Against Cyber Trespass Act,” prohibits deceptive practices related to spyware programs and requires notice and consent for the execution of information collection programs.

BACKGROUND AND NEED FOR LEGISLATION

The release of the Mosaic browser to the public in January 1993, which provided the first graphical interface for navigating the Internet, is credited with bringing the Internet into the mainstream of public usage. In less than one decade, Internet usage was transformed from an academic tool into a commercial, educational, and communications portal accessed by more than 70% of Americans. To accommodate the enormous growth in Internet use and to meet the needs of online consumers, the market has continually responded with new technologies tailored to consumer Internet usage.

Many of the technologies that have emerged are designed to improve the efficiency and speed of data transfer. Websites may use browsers to run program-like functions on the user’s computer, such as scripting and applets, to maximize server efficiency and thereby reduce time requirements for a web page to load on a user’s computer. Technology has also allowed websites to use persistent identifiers to recognize a return visitor, and thereby enhance the online experience through personalization. The unique nature of the Internet has also facilitated other beneficial technologies that capitalize on the distributed network structure. Peer-to-peer file sharing software, instant messaging, and voice-over Internet are but a few examples of the developments that benefit millions of users.

Accompanying the growth in available technologies are emerging concerns regarding harmful uses of these same technologies. The Committee is aware that the same beneficial technologies that provide benefits to millions of users can be applied in ways that present serious problems for consumers when misused by those with unsavory motives. The Committee is particularly concerned about the growing use of what is commonly referred to as spyware. Computer software known as “spyware” can allow the unscrupu-

lous to prey on unwitting consumers by stealing personal and financial information or exposing them to unsolicited offensive material. In many instances, spyware software downloads from the Internet are occurring without the computer user's knowledge and consent. The covert nature of the software installation makes it very difficult for a user to detect the presence of the software. In fact, when the software begins to degrade the function of the computer, consumers often confuse the true source of the spyware with the browser they are using or the particular application they are running. Many of the same programs prevent a user from properly or completely uninstalling or disabling the software program.

Spyware presents privacy, security, and functionality concerns for consumers. The Federal Trade Commission loosely defines "spyware" as software "that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge." The Committee received testimony that spyware represents a range of software programs on a broad continuum from the most pernicious criminal activities on one end to the less threatening but still intrusive on the opposite end of the spectrum.

The most serious privacy and security concerns pertain to those programs that are intended to capture a user's personal information without knowledge and consent. The Committee received testimony demonstrating the software technology and tactics of some of these programs. They include keystroke logging software that captures a user's information (passwords, social security numbers, account numbers, etc.) and can lead to identity theft, and monitoring software that tracks a user's online activity, such as websites visited. Such information could be used for profiling. In a related development, security experts and law enforcement officers report growing cooperation among spammers, virus writers, and con artists to steal millions of dollars from consumers through a device called "phishing" which captures passwords and other private financial data from consumers. Software can also impact the functioning of a computer by redirecting the user to websites the user does not intend to visit, preventing a user from altering settings on the computer, or using the computer to send unsolicited commercial electronic mail. The Committee is concerned that such attacks could erode the trust that makes electronic commerce and online banking possible.

Techniques for deceiving consumers into downloading spyware vary. Deceptive tactics include using pop-under windows that disguise the identity of the program distributor, offering misleading or deceptive end user licensing agreements, and failing to disclose the functionality of a program. More nefarious tactics include exploitation of security patches in a computer's operating system. Additionally, consumers who leave browser security settings on "low" open their systems to automatic "drive-by" downloads in which spyware programs are automatically downloaded when visiting certain websites.

Other software, known as adware, may not have the security risks associated with spyware but may raise significant privacy concerns. Adware is advertising software that can monitor online behavior and websites visited. Adware is often bundled with other

software a consumer voluntarily downloads. Often, the adware is consideration for otherwise free software a consumer chooses to download. This is known as freeware. The adware usually directs targeted advertisements to the user's computer based on information gathered about the user's online activity. However, some adware has been used to push directed advertisements of material unrelated to online activity that a user may find objectionable. The Committee does not find adware per se objectionable so long as a consumer has given informed consent to the software installation or execution.

The Committee recognizes that many of the technologies that are used for malicious and deceptive practices can also be used for beneficial and legitimate purposes. For example, parents utilizing software to monitor the online behavior of their children may find it to be an appropriate tool to protect their children. Similarly, software companies, Internet Service Providers, and other intermediaries may have legitimate business reasons to monitor and track activity. Examples include system performance, network efficiency, and automatic updates of anti-virus software. The Committee does not view the technology employed by spyware and adware as the source of the problem and therefore, does not seek to regulate the software. Rather, it is the misuse of this technology that has created significant policy concerns the Committee intends to address through this legislation and ongoing oversight.

HEARINGS

The Subcommittee on Commerce, Trade, and Consumer Protection held a hearing on spyware legislation on April 29, 2004. The Subcommittee received testimony from: The Honorable Mozelle W. Thompson, Commissioner, Federal Trade Commission; Mr. Howard Beales, Director, Bureau of Consumer Protection, Federal Trade Commission; Mr. Ari Schwartz, Associate Director, Center for Democracy and Technology; Mr. Dave Baker, Vice President for Law and Public Policy, EarthLink; and Mr. Jeffrey Friedberg, Director of Windows Privacy, Microsoft.

COMMITTEE CONSIDERATION

On Thursday, June 17, 2004, the Subcommittee on Commerce, Trade, and Consumer Protection met in open markup session and approved H.R. 2929 for Full Committee consideration, as amended, by a voice vote. On Thursday, June 24, 2004, the Committee on Energy and Commerce met in open markup session and ordered H.R. 2929 reported to the House, as amended, by a recorded vote of 45 yeas to 4 nays, a quorum being present.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto. The following is the recorded vote taken on the motion by Mr. Pickering to order H.R. 2929 reported to the House, as amended, which was agreed to by a recorded vote of 45 yeas to 4 nays.

COMMITTEE ON ENERGY AND COMMERCE -- 108TH CONGRESS
ROLL CALL VOTE # 73

BILL: H.R. 2929, Safeguard Against Privacy Invasions Act.

AMENDMENT: Motion by Mr. Pickering to order H.R. 2929 reported to the House, amended.

DISPOSITION: **AGREED TO**, by a roll call vote of 45 yeas to 4 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Mr. Barton				Mr. Dingell	X		
Mr. Tauzin				Mr. Waxman	X		
Mr. Hall	X			Mr. Markey	X		
Mr. Bilirakis	X			Mr. Boucher	X		
Mr. Upton	X			Mr. Towns	X		
Mr. Stearns	X			Mr. Pallone			
Mr. Gillmor	X			Mr. Brown	X		
Mr. Greenwood	X			Mr. Gordon	X		
Mr. Cox				Mr. Deutsch			
Mr. Deal	X			Mr. Rush	X		
Mr. Burr	X			Ms. Eshoo		X	
Mr. Whitfield	X			Mr. Stupak		X	
Mr. Norwood	X			Mr. Engel	X		
Mrs. Cubin				Mr. Wynn	X		
Mr. Shimkus	X			Mr. Green	X		
Mrs. Wilson	X			Ms. McCarthy	X		
Mr. Shadegg	X			Mr. Strickland		X	
Mr. Pickering	X			Ms. DeGette	X		
Mr. Fossella	X			Ms. Capps	X		
Mr. Buyer	X			Mr. Doyle	X		
Mr. Radanovich	X			Mr. John			
Mr. Bass	X			Mr. Allen	X		
Mr. Pitts	X			Mr. Davis	X		
Ms. Bono	X			Ms. Schakowsky	X		
Mr. Walden	X			Ms. Solis	X		
Mr. Terry	X			Mr. Gonzalez	X		
Mr. Ferguson	X						
Mr. Rogers							
Mr. Issa		X					
Mr. Otter	X						
Mr. Sullivan	X						

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held a legislative hearing and made findings that are reflected in this report.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

H.R. 2929 prohibits deceptive practices related to spyware programs and requires notice and consent for the execution of information collection programs.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 2929, the Securely Protect Yourself Against Cyber Trespass Act, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

COMMITTEE COST ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 8, 2004.

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

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 2929, the Securely Protect Yourself Against Cyber Trespass Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Melissa E. Zimmerman (for federal costs), Sarah Puro (for the impact on state, local, and tribal governments), and Paige Piper/Bach (for the private-sector impact).

Sincerely,

ELIZABETH M. ROBINSON
(For Douglas Holtz-Eakin, Director).

Enclosure.

H.R. 2929—Securely Protect Yourself Against Cyber Trespass Act

Summary: H.R. 2929 would prohibit the use of computer software (known as spyware) to collect personal information and to monitor the behavior of computer users without a user's consent. The Federal Trade Commission (FTC) would be directed to enforce

this bill's provisions relating to spyware, including assessing and collecting civil penalties for unfair or deceptive business practices. (Civil penalties are recorded in the federal budget as revenues.) Based on information provided by the FTC, CBO estimates that implementing H.R. 2929 would not have a significant effect on revenues or spending subject to appropriation. Enacting the bill would not affect direct spending.

H.R. 2929 contains both an intergovernmental mandates and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA). CBO estimates that the cost of the mandates would fall below the annual thresholds established by UMRA: \$60 million in 2004 for intergovernmental mandates, and \$120 million in 2004 for private-sector mandates. (Both thresholds are adjusted annually for inflation.)

Estimated cost to the Federal Government: Enacting H.R. 2929 could increase federal revenues from civil penalties assessed for committing unfair or deceptive acts or practices in commerce, but CBO estimates that any new collections would be less than \$500,000 a year.

Implementing the bill also could increase spending by the FTC for law enforcement, subject to the availability of appropriated funds. Based on information from the agency, CBO expects that any such increase would be insignificant.

Estimated impact on state, local, and tribal governments: Section 6 would preempt state laws that prohibit the use of certain types of computer software and establish penalties for violators. This preemption constitutes a mandate as defined in UMRA. Utah has already passed legislation that this bill would preempt, and California, Iowa, and New York have bills pending before their state legislatures. However, the preemption is narrow and the bill would specifically preserve state authority to pursue fraud, trespass, contract, and tort cases under state law. CBO estimates that any costs to state, local, or tribal governments would be minimal and would fall significantly below the threshold established in UMRA (\$60 million in 2004, adjusted annually for inflation).

Estimated impact on the private sector: H.R. 2929 would impose private-sector mandates, as defined in UMRA, on persons who use computer programs to collect certain information from another person's computer. Based on information provided by industry and government sources, CBO expects that the direct costs of complying with those mandates would fall below the annual threshold established by UMRA for private-sector mandates (\$120 million in 2004, adjusted annually for inflation).

The bill would require a person who transmits or executes an information collection program on someone's computer to receive prior consent from the owner or authorized user of that computer. An information collection program is defined in the legislation as computer software that collects personally identifiable information and sends the information to someone else or collects Web tracking information and uses such information for advertising purposes. The bill would require the Federal Trade Commission to provide the manner and form of the notice to obtain consent. In addition, the bill would require an information collection program installed on someone's computer to be easily identifiable and removable.

Estimate prepared by: Federal Costs: Melissa E. Zimmerman. Impact on State, Local, and Tribal Governments: Sarah Puro. Impact on the Private Sector: Paige Piper/Bach.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause 3, which grants Congress the power to regulate commerce with foreign nations, among the several states, and with the Indian tribes.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

Section 1 establishes the short title of the Act as the “Securely Protect Yourself Against Cyber Trespass Act,” or the “SPY ACT.”

Section 2. Prohibition of deceptive acts or practices relating to spyware

Section 2(a) prohibits any person who is not an owner or authorized user of a protected computer to engage in deceptive acts or practices in connection with spyware. Specifically it prohibits deceptively: taking control of a protected computer; modifying settings related to the use of a computer or to the computer’s access to or use of the Internet by altering certain information; collecting personally identifiable information through the use of a keystroke logging function or similar function; 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; 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; 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; inducing the owner or authorized user to provide personally identifiable information to

another person by misrepresenting the identity or authority of the person seeking the information; removing, disabling, or rendering inoperative a security, anti-spyware, or anti-virus technology installed on the computer, or 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 section 2.

The Committee notes that it has preserved and expects that the Federal Trade Commission (FTC) will use its authority to issue advisory opinions, policy statements, and guidance to advise companies on the parameters of this section. For example the FTC should issue guidance on required disclosures or material omissions that would trigger liability under section 2.

Many software installations of updated security, anti-spyware, or anti-virus technologies requested by a computer user will disable or render inoperable a prior version of that software upon installation of the updated version. Section 2(a)(8) is not intended to apply to these circumstances.

Section 2(b) provides that the section shall take effect on the date of enactment of the Act.

Section 3. Prohibition of collection of certain information without notice and consent

Section 3(a) prohibits the transmission of an information collection program to a protected computer unless the program provides for notice and consent before the first execution of the information collection program and contains the functions set forth in section 3(d). It also prohibits the execution of any information collection program on a protected computer without the consent of the owner or authorized user.

This section contemplates a single notice at the first execution of the software. If the same information collection program executes more than one time on the same protected computer, notice is required only at the initial execution. Subsequent notice is only required if the information collection program will collect or send information that is materially different from, and outside the scope of, the type or purpose set forth in the initial or, in the case of prior subsequent notice, previous notice.

Section 3(b) provides a definition for information collection program. An information collection program is computer software that (a) collects personally identifiable information and either (1) sends such information to a person other than the owner or authorized user of the computer or (2) uses such information to deliver advertising to or display advertising on the computer; or (b) collects information regarding web pages accessed using the computer and uses the information to deliver advertising to or display advertising on the computer. The reference to “a person other than the owner or authorized user of the computer” in Section 3(b)(1)(B)(i) is intended to include the entity that transmitted or executed the information collection program.

Section 3(c) sets out the requirements for notice and consent with respect to information collection programs. The notice must be clear and conspicuous in plain language and clearly distinguished from any other information contemporaneously displayed. Section 3(c)(1)(A) is not intended to impose design mandates on hardware

manufacturers or software developers. The intent of the provision is to require a clearly distinct notice to the extent practicable in light of the technical and functional limitations of the information collection program or the device on which it is installed and executed. The notice must also contain a statement identifying whether the information collection program collects personally identifiable information or web pages accessed or both. The provider of the information collection program may use the provided language or substantially similar language. The language “or substantially similar language” has been added to section 3(c)(1)(B) to ensure that vendors of information collection programs have adequate flexibility to tailor section 3 notices to the user experience and in light of evolving technologies and consumer expectations. The notice must provide for the user to grant or deny consent. The notice must also provide for the user to access, before granting or denying consent, a clear description of the types of information being collected, the purpose for which the information is being collected and sent, and in the case of bundled software, the identity of the programs that qualify as information collection programs under the Act. The software provider may provide access to the information required under section 3(c)(1)(D) by a link or some other web-based mechanism. A single notice is sufficient for bundled software programs so long as it meets the requirements under section 3(c)(1)(D)(iii). Section 3(c)(1)(E) requires concurrent display of the specified information in sections 3(c)(1)(B), (C), and (D) to the extent reasonably practicable. Section 3(c) grants the FTC authority to issue regulations to carry out the subsection.

Section 3(d) provides that an information collection program must contain a disable function and, if applicable, an identity function. The disable function must allow a user of the program to remove or disable operation of the program by a mechanism that is easily identifiable to the user and can be performed without undue effort or knowledge by the user of the protected computer. Section 3(d)(1) does not require information collection programs to provide users with both a remove and a disable option. Developers of information collection programs will satisfy the requirements of Section 3(d)(1) so long as the program includes at least one of these options. The identity function must be included in any information collection program that delivers advertising to or displays advertising on a protected computer. The function must provide that display of an advertisement generated by information collected through the program must be accompanied by a statement that identifies the information collection program. Section 3(d) gives the FTC authority to issue regulations to carry out the subsection.

Section 3(e) provides that a telecommunications carrier, provider of information or interactive computer service, cable operator, or a provider of transmission capability shall not be liable under section 3 to the extent that it transmits, routes, hosts, stores, or provides connections for an information collection program or provides an information location tool through which the owner or authorized user of a protected computer locates an information collection program.

Section 4. Enforcement

Section 4(a) provides that the Act shall be enforced by the FTC under the Federal Trade Commission Act and that a violation of the 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 except that the civil penalties for a violation of the Act are as set forth in this section. Accordingly, the Committee intends that the standard for FTC enforcement of a civil action to recover a civil monetary penalty in a district court of the United States in a case of a violation of this Act shall be, as provided in section 5(m)(1)(A) of the Federal Trade Commission Act, “actual knowledge or knowledge fairly implied on the basis of objective circumstances” that the conduct is unfair and deceptive and is prohibited by this Act. Similarly, the Committee intends that section 5(m)(1)(B) of the Federal Trade Commission Act will apply in such circumstances to require the court, in determining the amount of any such civil penalty for violation of this Act, to 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.” The Committee expects the FTC, before it seeks any damages under this Act, to formulate and make public guidance on the standards it intends to apply in determining the amount of civil penalties it will seek.

The section gives the FTC the discretion to seek civil penalties for violations of the Act in one of two ways: (1) by treating conduct affecting multiple computers as separate violations, with damages up to \$33,000 for each violation of section 2 and \$11,000 for each violation of section 3; or (2) by treating conduct affecting multiple computers as a single violation with damages up to \$3,000,000 for each violation of section 2 and \$1,000,000 for each violation of section 3. Any single action or conduct that violates more than one provision of section 2(a) shall be considered multiple violations based on the number of paragraphs violated. The Committee expects the FTC to vigorously enforce the law to protect consumers from unfair or deceptive acts or practices involving spyware. It also expects the agency to act reasonably to avoid seeking damages out of proportion to the harm caused by the offending conduct.

Section 4(b) provides that remedies available under this section and remedies available under the Federal Trade Commission Act are the exclusive remedies for violation of the Act.

Section 4(c) provides that the section shall take effect on the date of enactment of the Act to the extent that the section applies to violations of section 2(a).

Section 5. Limitations

Section 5(a) provides that sections 2 and 3 of the Act shall not apply to any act taken by a law enforcement agent in performance of official duties or 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 in response to a request or demand made under authority granted to that agency or department.

Section 5(b) provides that nothing in the Act shall apply to any monitoring of, or interaction with, a subscriber’s Internet or other network connection or service by a telecommunications carrier,

cable operator, or provider of information service or interactive computer service for network security purposes, diagnostics or repair in connection with a network or service, or detection or prevention of fraudulent activities in connection with a service or a user agreement.

Section 5(c) provides that no provider of an interactive computer service may be held liable under the 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 and installed on a customer's computer, if the provider notifies the customer and obtains consent before undertaking such action.

Section 6. Effect on other laws

Section 6(a) provides that the Act supercedes any provision of a statute, regulation, or rule of a state or political subdivision that expressly regulates deceptive conduct with respect to computers similar to that of section 2(a), the transmission or execution of a computer program similar to that in section 3, and the use of context based triggering mechanisms to display advertisement that partially or wholly cover or obscure content on a web page. The section specifically preserves state trespass, contract and tort law, and other state laws to the extent those acts relate to acts of consumer fraud and deceptive practices generally. The Committee intends to preserve the ability of State Attorneys General to enforce these laws as an important backstop to FTC enforcement of this Act and the Federal Trade Commission Act. However, the Committee intends to preempt state legislation that makes illegal an information collection program or other context based triggering mechanism that complies with this Act by simply calling it a trespass, tort or other statute in an effort to avoid preemption. The Committee specifically intends to preempt the Utah Spyware Control Act, Section 13-39-101, Utah Code Annotated 1953.

Section 6(b) preserves the Federal Trade Commission's authority to issue advisory opinions, policy statements, or guidance regarding the Act.

Section 7. Annual FTC report

Section 7 requires the Federal Trade Commission to submit annual reports to Congress. The report must detail the actions taken to enforce sections 2(a) and 3 and describe administrative structure and personnel and other resources committed to enforcement of the Act.

Section 8. Regulations

Section 8 provides that any regulations issued under the Act shall be issued in accordance with section 553 of title 5, United States Code. Initial regulations shall be issued no later than six months from date of enactment of the Act.

Section 9. Definitions

Section 9 provides definitions for terms in the Act including "computer software," "deceptive acts or practices," "disable," "personally identifiable information," and "transmit."

The definition of "collect" makes clear that personally identifiable information that is input by the user of a protected computer and

transferred to the intended recipient is outside the scope of section 3 of the Act. This is intended to facilitate ease of use for consumers and providers of Internet services or websites.

Section 10. Applicability and sunset

Section 10 provides that, except as otherwise provided in the Act, the Act shall take effect 12 months after the date of enactment. Section 10 also provides for a sunset of the bill on December 31, 2009.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation does not amend any existing Federal statute.

EXCHANGE OF COMMITTEE CORRESPONDENCE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC, July 13, 2004.

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

DEAR CHAIRMAN BARTON: On June 25, 2004, I wrote to Speaker Hastert to request a sequential referral of H.R. 2929, the "Safeguard Against Privacy Invasions Act."

My request was based on two provisions, one of which was in the introduced bill and one of which was in an amendment adopted at committee. I understand that neither of these two provisions will be included in the bill that will be reported to the House. I further understand that the Speaker's policy is not to grant sequential referrals when the provisions on which the sequential referral request is based have been removed from the bill that will be reported to the House. Given that policy, I will not pursue the sequential referral further.

I appreciate your cooperation in this matter.

Sincerely,

F. JAMES SENSENBRENNER, Jr.,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC, July 13, 2004.

Hon. F. JAMES SENSENBRENNER Jr.,
*Chairman, Committee on the Judiciary, House of Representatives,
Rayburn House Office Building, Washington, DC.*

DEAR CHAIRMAN SENSENBRENNER: I am writing to confirm that the two provisions you made reference to in your June 25, 2004 letter to Speaker Hastert on H.R. 2929, the Safeguard Against Privacy Invasions Act, will not be included in the bill to be reported by the Committee on Energy and Commerce.

I appreciate your cooperation in these matters as we work to bring this bill to the House floor.
Sincerely,

JOE BARTON,
Chairman.

○