Union Calendar No. 374

108TH CONGRESS
2D SESSION

H. R. 2929

[Report No. 108–619]

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

IN THE HOUSE OF REPRESENTATIVES

JULY 25, 2003

Mrs. BONO (for herself and Mr. TOWNS) introduced the following bill; which was referred to the Committee on Energy and Commerce

JULY 20, 2004

Additional sponsors: Mr. SHIMKUS, Mrs. CUBIN, Mr. EHLERS, Mr. CALVERT, Mr. BUYER, Mr. RADANOVICH, Mr. PICKERING, Mr. WYNN, Mr. ENGEL, Mr. RUSH, Mr. BOUCHER, Mr. STUPAK, Mr. GREEN of Texas, Mr. GORDON, Mr. DEUTSCH, Ms. MCCARTHY of Missouri, Mr. GILLMOR, Mr. HALL, Mr. SHADEGG, Mr. BASS, Mr. GREENWOOD, Mr. GONZALEZ, Mr. WAMP, Mr. OTTER, Mr. DOOLITTLE, Mr. UPTON, Mr. BURNS, Mr. ISRAEL, Mr. SAM JOHNSON of Texas, and Mr. BRADLEY of New Hampshire

JULY 20, 2004

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in italic]

[For text of introduced bill, see copy of bill as introduced on July 25, 2003]

A BILL

To protect users of the Internet from unknowing trans-

mission of their personally identifiable information through spyware programs, and for other purposes.

1   *Be it enacted by the Senate and House of Representa-*

2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4   *This Act may be cited as the "Securely Protect Yourself*

5 *Against Cyber Trespass Act" or the "SPY ACT".*

6 **SEC. 2. PROHIBITION OF DECEPTIVE ACTS OR PRACTICES**

7   **RELATING TO SPYWARE.**

8   *(a) PROHIBITION.—It is unlawful for any person, who*

9 *is not the owner or authorized user of a protected computer,*

10 *to engage in deceptive acts or practices in connection with*

11 *any of the following conduct with respect to the protected*

12 *computer:*

13   *(1) Taking control of the computer by—*

14   *(A) utilizing such computer to send unsolic-*

15   *ited information or material from the protected*

16   *computer to others;*

17   *(B) diverting the Internet browser of the*

18   *computer, or similar program of the computer*

19   *used to access and navigate the Internet, away*

20   *from the site the user intended to view, to one or*

21   *more other Web pages, such that the user is pre-*

22   *vented from viewing the content at the intended*

23   *Web page;*

1   *(C) accessing or using the modem, or Inter-*

2 *net connection or service, for the computer and*

3 *thereby causing damage to the computer or caus-*

4 *ing the owner or authorized user to incur unau-*

5 *thorized financial charges;*

6   *(D) using the computer as part of an activ-*

7 *ity performed by a group of computers that*

8 *causes damage to another computer; or*

9   *(E) delivering advertisements that a user of*

10 *the computer cannot close without turning off the*

11 *computer or closing all sessions of the Internet*

12 *browser for the computer.*

13 *(2) Modifying settings related to use of the com-*

14 *puter or to the computer's access to or use of the*

15 *Internet by altering—*

16   *(A) the Web page that appears when the*

17 *owner or authorized user launches an Internet*

18 *browser or similar program used to access and*

19 *navigate the Internet;*

20   *(B) the default provider used to access or*

21 *search the Internet, or other existing Internet*

22 *connections settings;*

23   *(C) a list of bookmarks used by the com-*

24 *puter to access Web pages; or*

1   *(D) security or other settings of the com-*

2   *puter that protect information about the owner*

3   *or authorized user.*

4   *(3) Collecting personally identifiable information*

5   *through the use of a keystroke logging function or*

6   *similar function.*

7   *(4) Inducing the owner or authorized user to in-*

8   *stall a computer software component onto the com-*

9   *puter, or preventing reasonable efforts to block the in-*

10   *stallation or execution of, or to disable, a computer*

11   *software component by—*

12   *(A) presenting the owner or authorized user*

13   *with an option to decline installation of a soft-*

14   *ware component such that, when the option is se-*

15   *lected by the owner or authorized user, the in-*

16   *stallation nevertheless proceeds; or*

17   *(B) causing a computer software component*

18   *that the owner or authorized user has properly*

19   *removed or disabled to automatically reinstall or*

20   *reactivate on the computer.*

21   *(5) Misrepresenting that installing a separate*

22   *software component or providing log-in and password*

23   *information is necessary for security or privacy rea-*

24   *sons, or that installing a separate software component*

1   *is necessary to open, view, or play a particular type*

2   *of content.*

3   *(6) Inducing the owner or authorized user to in-*

4   *stall or execute computer software by misrepresenting*

5   *the identity or authority of the person or entity pro-*

6   *viding the computer software to the owner or user.*

7   *(7) Inducing the owner or authorized user to*

8   *provide personally identifiable information to another*

9   *person by misrepresenting the identity or authority of*

10   *the person seeking the information.*

11   *(8) Removing, disabling, or rendering inoper-*

12   *ative a security, anti-spyware, or anti-virus tech-*

13   *nology installed on the computer.*

14   *(9) Installing or executing on the computer one*

15   *or more additional computer software components*

16   *with the intent of causing a person to use such com-*

17   *ponents in a way that violates any other provision of*

18   *this section.*

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

20   *on the date of the enactment of this Act.*

21   **SEC. 3. PROHIBITION OF COLLECTION OF CERTAIN INFOR-**

22   **MATION WITHOUT NOTICE AND CONSENT.**

23   *(a) OPT-IN REQUIREMENT.—Except as provided in*

24   *subsection (e), it is unlawful for any person—*

1   *(1) to transmit to a protected computer, which*

2   *is not owned by such person and for which such per-*

3   *son is not an authorized user, any information collec-*

4   *tion program, or*

5   *(2) to execute any information collection pro-*

6   *gram installed on such a protected computer,*

7 *unless, before the first execution of any of the information*

8 *collection functions of the program, the owner or an author-*

9 *ized user of the protected computer has consented to such*

10 *execution pursuant to notice in accordance with subsection*

11 *(c) and such information collection program includes the*

12 *functions required under subsection (d).*

13   *(b) INFORMATION COLLECTION PROGRAM.—For pur-*

14 *poses of this section, the term "information collection pro-*

15 *gram" means computer software that—*

16   *(1)(A) collects personally identifiable informa-*

17   *tion; and*

18   *(B)(i) sends such information to a person other*

19   *than the owner or authorized user of the computer, or*

20   *(ii) uses such information to deliver advertising*

21   *to, or display advertising, on the computer; or*

22   *(2)(A) collects information regarding the Web*

23   *pages accessed using the computer; and*

24   *(B) uses such information to deliver advertising*

25   *to, or display advertising on, the computer.*

1 *(c) NOTICE AND CONSENT.—*

2   *(1) IN GENERAL.—Notice in accordance with this*

3 *subsection with respect to an information collection*

4 *program is clear and conspicuous notice in plain lan-*

5 *guage, set forth in a form and manner as the Com-*

6 *mission shall provide, that meets all of the following*

7 *requirements:*

8   *(A) The notice clearly distinguishes such no-*

9 *tice from any other information visually pre-*

10 *sented contemporaneously on the protected com-*

11 *puter.*

12   *(B) The notice contains one of the following*

13 *statements, as applicable, or substantially simi-*

14 *lar language:*

15   *(i) With respect to an information col-*

16 *lection program described in subsection*

17 *(b)(1): "This program will collect and*

18 *transmit information about you. Do you ac-*

19 *cept?".*

20   *(ii) With respect to an information col-*

21 *lection program described in subsection*

22 *(b)(2): "This program will collect informa-*

23 *tion about Web pages you access and will*

24 *use that information to display advertising*

25 *on your computer. Do you accept?".*

8

(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

1   *the information collection functions of the*

2   *program together with the first execution of*

3   *other computer software, the identity of any*

4   *such software that is an information collec-*

5   *tion program.*

6   *(E) The notice provides for concurrent dis-*

7   *play of the information required under subpara-*

8   *graphs (B) and (C) and the option required*

9   *under subparagraph (D) until the user grants or*

10   *denies consent using the option required under*

11   *subparagraph (C) (or selects the option required*

12   *under subparagraph (D)).*

13   *(2) SINGLE NOTICE.—The Commission shall pro-*

14   *vide that, in the case in which multiple information*

15   *collection programs first execute any of the informa-*

16   *tion collection functions of the programs together, no-*

17   *tice in accordance with paragraph (1) may be pro-*

18   *vided through a single notice that applies to all such*

19   *information collection programs, except that such no-*

20   *tice shall provide the option under subparagraph (D)*

21   *of paragraph (1) with respect to each such informa-*

22   *tion collection program.*

23   *(3) CHANGE IN INFORMATION COLLECTED.—*

24   *After an owner or authorized user has granted con-*

25   *sent to execution of an information collection pro-*

1 gram pursuant to a notice in accordance with this

2 subsection, the person who transmitted the program

3 shall provide another notice in accordance with this

4 subsection and obtain consent before such program

5 may be used to collect or send information of any

6 type or for any purpose that is materially different

7 from, and outside the scope of, the type or purpose set

8 forth in the initial or any previous notice.

9   (4) REGULATIONS.—The Commission shall issue

10 regulations to carry out this subsection.

11 (d) REQUIRED FUNCTIONS.—The functions required

12 under this subsection to be included in an information col-

13 lection program that first executes any information collec-

14 tion functions with respect to a protected computer are as

15 follows:

16   (1) DISABLING FUNCTION.—With respect to any

17   information collection program, a function of the pro-

18   gram that allows a user of the program to remove the

19   program or disable operation of the program with re-

20   spect to such protected computer by a function that—

21   (A) is easily identifiable to a user of the

22   computer; and

23   (B) can be performed without undue effort

24   or knowledge by the user of the protected com-

25   puter.

1   *The Commission may issue regulations to carry out*

2   *this paragraph.*

3   *(2) IDENTITY FUNCTION.—With respect only to*

4   *an information collection program that uses informa-*

5   *tion collected in the manner described in paragraph*

6   *(1)(B)(ii) or (2)(B) of subsection (b), a function of the*

7   *program that provides that each display of an adver-*

8   *tisement directed or displayed using such information*

9   *is accompanied by a statement that clearly identifies*

10   *the information collection program.*

11   *(e) LIMITATION ON LIABILITY.—A telecommunications*

12 *carrier, a provider of information service or interactive*

13 *computer service, a cable operator, or a provider of trans-*

14 *mission capability shall not be liable under this section to*

15 *the extent that the carrier, operator, or provider—*

16   *(1) transmits, routes, hosts, stores, or provides*

17   *connections for an information collection program*

18   *through a system or network controlled or operated by*

19   *or for the carrier, operator, or provider; or*

20   *(2) provides an information location tool, such*

21   *as a directory, index, reference, pointer, or hypertext*

22   *link, through which the owner or user of a protected*

23   *computer locates an information collection program.*

1 *SEC. 4. ENFORCEMENT.*

2 *(a) UNFAIR OR DECEPTIVE ACT OR PRACTICE.—This*

3 *Act shall be enforced by the Commission under the Federal*

4 *Trade Commission Act (15 U.S.C. 41 et seq.). A violation*

5 *of any provision of this Act or of a regulation issued under*

6 *this Act shall be treated as an unfair or deceptive act or*

7 *practice violating a rule promulgated under section 18 of*

8 *the Federal Trade Commission Act (15 U.S.C. 57a), except*

9 *that the maximum civil penalty for a violation of this Act*

10 *shall be one of the following amounts, as the Commission,*

11 *in its discretion, seeks for such a violation:*

12 *(1) TREATMENT OF CONDUCT AFFECTING MUL-*

13 *TIPLE COMPUTERS AS SEPARATE VIOLATIONS.—*

14 *$33,000 for each violation of section 2, and $11,000*

15 *for each violation of section 3, except that in applying*

16 *this paragraph each separate protected computer with*

17 *respect to which a violation of such section occurs as*

18 *a result of a single action or conduct that violates sec-*

19 *tion 2 or 3 shall be treated as a separate violation.*

20 *(2) TREATMENT OF CONDUCT AFFECTING MUL-*

21 *TIPLE COMPUTERS AS A SINGLE VIOLATION.—*

22 *$3,000,000 for each violation of section 2, and*

23 *$1,000,000 for each violation of section 3, except that*

24 *in applying this paragraph—*

25 *(A) any single action or conduct that vio-*

26 *lates such section with respect to multiple pro-*

1   *tected computers shall be treated as a single vio-*

2   *lation; and*

3   *(B) any single action or conduct that vio-*

4   *lates more than one paragraph of section 2(a)*

5   *shall be considered multiple violations, based on*

6   *the number of such paragraphs violated.*

7   *(b) EXCLUSIVENESS OF REMEDIES.—The remedies in*

8   *this section (including remedies available under the Federal*

9   *Trade Commission Act) are the exclusive remedies for viola-*

10   *tions of this Act.*

11   *(c) EFFECTIVE DATE.—This section shall take effect*

12   *on the date of the enactment of this Act, but only to the*

13   *extent that this section applies to violations of section 2(a).*

14   **SEC. 5. LIMITATIONS.**

15   *(a) LAW ENFORCEMENT AUTHORITY.—Sections 2 and*

16   *3 of this Act shall not apply to—*

17   *(1) any act taken by a law enforcement agent in*

18   *the performance of official duties; or*

19   *(2) the transmission or execution of an informa-*

20   *tion collection program in compliance with a law en-*

21   *forcement, investigatory, national security, or regu-*

22   *latory agency or department of the United States in*

23   *response to a request or demand made under author-*

24   *ity granted to that agency or department, including*

25   *a warrant issued under the Federal Rules of Criminal*

1   *Procedure, an equivalent State warrant, a court*

2   *order, or other lawful process.*

3   *(b) EXCEPTION RELATING TO NETWORK SECURITY.—*

4 *Nothing in this Act shall apply to any monitoring of, or*

5 *interaction with, a subscriber's Internet or other network*

6 *connection or service by a telecommunications carrier, cable*

7 *operator, or provider of information service or interactive*

8 *computer service for network security purposes, diagnostics*

9 *or repair in connection with a network or service, or detec-*

10 *tion or prevention of fraudulent activities in connection*

11 *with a service or user agreement.*

12   *(c) GOOD SAMARITAN PROTECTION.—No provider of*

13 *computer software or of interactive computer service may*

14 *be held liable under this Act on account of any action volun-*

15 *tarily taken, or service provided, in good faith to remove*

16 *or disable a program used to violate section 2 or 3 that*

17 *is installed on a computer of a customer of such provider,*

18 *if such provider notifies the customer and obtains the con-*

19 *sent of the customer before undertaking such action or pro-*

20 *viding such service.*

21 **SEC. 6. EFFECT ON OTHER LAWS.**

22   *(a) PREEMPTION OF STATE LAW.—*

23   *(1) PREEMPTION.—This Act supersedes any pro-*

24   *vision of a statute, regulation, or rule of a State or*

1 *political subdivision of a State that expressly regu-*

2 *lates—*

3   *(A) deceptive conduct with respect to com-*

4   *puters similar to that described in section 2(a);*

5   *(B) the transmission or execution of a com-*

6   *puter program similar to that described in sec-*

7   *tion 3; or*

8   *(C) the use of context-based triggering mech-*

9   *anisms or similar means to display an adver-*

10   *tisement that partially or wholly covers or ob-*

11   *scures content on a Web page in a way that*

12   *interferes with the ability of the user of a com-*

13   *puter to view the Web page.*

14   *(2) PROTECTION OF CERTAIN STATE LAWS.—*

15 *This Act shall not be construed to preempt the appli-*

16 *cability of—*

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

18   *(B) other State laws to the extent that those*

19   *laws relate to acts of fraud.*

20 *(b) PRESERVATION OF FTC AUTHORITY.—Nothing in*

21 *this Act may be construed in any way to limit or affect*

22 *the Commission's authority under any other provision of*

23 *law, including the authority to issue advisory opinions*

24 *(under Part 1 of Volume 16 of the Code of Federal Regula-*

25 *tions), 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　　　　*(1) CABLE OPERATOR.—The term "cable oper-*

2　*ator" has the meaning given such term in section 602*

3　*of the Communications Act of 1934 (47 U.S.C. 522).*

4　　　　*(2) COLLECT.—The term "collect" means, with*

5　*respect to information and for purposes only of sec-*

6　*tion 3, to obtain in a manner other than by transfer*

7　*by an owner or authorized user of a protected com-*

8　*puter to the party intended as recipient of the trans-*

9　*ferred information.*

10　　　　*(3) COMPUTER; PROTECTED COMPUTER.—The*

11　*terms "computer" and "protected computer" have the*

12　*meanings given such terms in section 1030(e) of title*

13　*18, United States Code.*

14　　　　*(4) COMPUTER SOFTWARE.—*

15　　　　　　*(A) IN GENERAL.—Except as provided in*

16　　　　*subparagraph (B), the term "computer software"*

17　　　　*means a set of statements or instructions that*

18　　　　*can be installed and executed on a computer for*

19　　　　*the purpose of bringing about a certain result.*

20　　　　　　*(B) EXCEPTION FOR COOKIES.—Such term*

21　　　　*does not include a cookie or other text file, data,*

22　　　　*or computer software, that is placed on the com-*

23　　　　*puter system of a user by an Internet service*

24　　　　*provider, interactive computer service, or Inter-*

25　　　　*net website to return information to such pro-*

1   *vider, service, or website solely to enable the user*

2   *subsequently to use such provider or service or to*

3   *access such website.*

4   *(5) COMMISSION.—The term "Commission"*

5   *means the Federal Trade Commission.*

6   *(6) DAMAGE.—The term "damage" has the*

7   *meaning given such term in section 1030(e) of title*

8   *18, United States Code.*

9   *(7) DECEPTIVE ACTS OR PRACTICES.—The term*

10   *"deceptive acts or practices" has the meaning appli-*

11   *cable to such term for purposes of section 5 of the*

12   *Federal Trade Commission Act (15 U.S.C. 45).*

13   *(8) DISABLE.—The term "disable" means, with*

14   *respect to an information collection program, to per-*

15   *manently prevent such program from executing any*

16   *of the functions described in section 3(b) that such*

17   *program is otherwise capable of executing (including*

18   *by removing, deleting, or disabling the program), un-*

19   *less the owner or operator of a protected computer*

20   *takes a subsequent affirmative action to enable the*

21   *execution of such functions.*

22   *(9) INFORMATION COLLECTION FUNCTIONS.—The*

23   *term "information collection functions" means, with*

24   *respect to an information collection program, the*

1 *functions of the program described in subsection (b)*

2 *of section 3.*

3 *(10) INFORMATION SERVICE.—The term "infor-*

4 *mation service" has the meaning given such term in*

5 *section 3 of the Communications Act of 1934 (47*

6 *U.S.C. 153).*

7 *(11) INTERACTIVE COMPUTER SERVICE.—The*

8 *term "interactive computer service " has the meaning*

9 *given such term in section 230(f) of the Communica-*

10 *tions Act of 1934 (47 U.S.C. 230(f)).*

11 *(12) INTERNET.—The term "Internet" means*

12 *collectively the myriad of computer and telecommuni-*

13 *cations facilities, including equipment and operating*

14 *software, which comprise the interconnected world-*

15 *wide network of networks that employ the Trans-*

16 *mission Control Protocol/Internet Protocol, or any*

17 *predecessor or successor protocols to such protocol, to*

18 *communicate information of all kinds by wire or*

19 *radio.*

20 *(13) PERSONALLY IDENTIFIABLE INFORMA-*

21 *TION.—*

22 *(A) IN GENERAL.—The term "personally*

23 *identifiable information" means the following in-*

24 *formation, to the extent only that such informa-*

1   *tion allows a living individual to be identified*

2   *from that information:*

3   *(i) First and last name of an indi-*

4   *vidual.*

5   *(ii) A home or other physical address*

6   *of an individual, including street name,*

7   *name of a city or town, and zip code.*

8   *(iii) An electronic mail address.*

9   *(iv) A telephone number.*

10   *(v) A social security number, tax iden-*

11   *tification number, passport number, driver's*

12   *license number, or any other government-*

13   *issued identification number.*

14   *(vi) A credit card number.*

15   *(vii) An account number.*

16   *(viii) Any access code or password,*

17   *other than an access code or password*

18   *transmitted by an owner or authorized user*

19   *of a protected computer to register for, or*

20   *log onto, a Web page or other Internet serv-*

21   *ice that is protected by an access code or*

22   *password.*

23   *(ix) Date of birth, birth certificate*

24   *number, or place of birth of an individual,*

1   *except in the case of a date of birth required*

2   *by law to be transmitted or collected.*

3   *(B) RULEMAKING.—The Commission may,*

4   *by regulation, add to the types of information*

5   *specified under paragraph (1) that shall be con-*

6   *sidered personally identifiable information for*

7   *purposes of this Act, except that such informa-*

8   *tion may not include any record of aggregate*

9   *data that does not identify particular persons,*

10   *particular computers, particular users of com-*

11   *puters, or particular email addresses or other lo-*

12   *cations of computers with respect to the Internet.*

13   *(14) TELECOMMUNICATIONS CARRIER.—The term*

14 *"telecommunications carrier" has the meaning given*

15 *such term in section 3 of the Communications Act of*

16 *1934 (47 U.S.C. 153).*

17   *(15) TRANSMIT.—The term "transmit" means,*

18 *with respect to an information collection program,*

19 *transmission by any means.*

20   *(16) WEB PAGE.—The term "Web page" means*

21 *a location, with respect to the World Wide Web, that*

22 *has a single Uniform Resource Locator or another*

23 *single location with respect to the Internet, as the*

24 *Federal Trade Commission may prescribe.*

1 ***SEC. 10. APPLICABILITY AND SUNSET.***

2   *(a) EFFECTIVE DATE.—Except as specifically pro-*

3 *vided otherwise in this Act, this Act shall take effect upon*

4 *the expiration of the 12-month period that begins on the*

5 *date of the enactment of this Act.*

6   *(b) APPLICABILITY.—Section 3 shall not apply to an*

7 *information collection program installed on a protected*

8 *computer before the effective date under subsection (a) of*

9 *this section.*

10   *(c) SUNSET.—This Act shall not apply after December*

11 *31, 2009.*

Union Calendar No. 374

108TH CONGRESS
2D SESSION

H. R. 2929

[Report No. 108–619]

A BILL

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

JULY 20, 2004

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed