fair project on solar energy. That was back in 1980. We saw, unfortunately, though, that the interest in alternative energy really dropped off after that time. Not only interest, but then Federal funding dropped off.

□ 1210

Just in talking to the Science Coalition this morning, they talked about how critical that was when that research funding dropped off. We can't afford to let that happen again. But what did happen with me is it really inspired me, got me interested. I went out and got a degree in mechanical engineering, and although I did not continue down that road, today I bring that background to this House and continue to work on these issues, understanding the importance of this issue and understanding the importance of the Federal Government's really investing in our future and especially in alternative energy. And these challenges are great. We must really confront them.

So today maybe this H-Prize Act will inspire another child out there today. He or she may become an engineer or a scientist or an entrepreneur who plays a hand in the next technological breakthrough. So there is great hope with this H-Prize Act. And today, Mr. Speaker, I ask my colleagues to join me by passing this bill, and hopefully in the future we can look back to today and see it as a major change and a major move forward for America and for the world.

Ms. EDDIE BERNICE JOHNSON of Texas. Mr. Speaker, I rise in support of H.R. 632, the H-Prize Act of 2007.

The federal government should become more involved in supporting cutting-edge technologies to reduce greenhouse gas emissions and move our nation toward renewable energy.

As a member of the House Committee on Science and Technology, I committed toward supporting a variety of renewable energy technologies—including hydrogen.

H.R. 632 would create competitive cash prizes to reward innovative research, development commercial application of hydrogen energy technologies.

Hydrogen cars and other vehicles would make such a difference in air quality, Mr. Speaker, especially in Texas. Cities in Texas have some of the poorest air quality in the Nation.

Hydrogen-powered vehicles could be designed for mass-scale use. These vehicles would emit only water vapor as a byproduct and reduce our dependence on foreign oil in the long term.

Hydrogen, solar, wind, geothermal, and nuclear are all cleaner energy sources than fossil fuels. H.R. 632 is a positive step toward developing energy technologies that create a brighter future for our children and grandchildren.

Mr. LARSON of Connecticut. Mr. Speaker, I rise today in support of the H-Prize Act of 2007, H.R. 632, an important step forward in making America more competitive and energy independent. As a founding member of the House Hydrogen and Fuel Cell Caucus and a cosponsor of this bill, I believe we must move forward in fostering innovation and competition in hydrogen technology, in order to end our addiction to oil.

According to the Department of Energy, major advances must be made in hydrogen production, distribution, and storage before it can be widely used as a fuel source. The H-Prize Act would excite and attract innovators throughout the country to take up this important task. Specifically, the bill would authorize $50 million from fiscal year 2008 through fiscal year 2017 to be awarded in cash prizes to non-federal entities in three categories—technologies created to assist in the distribution or production of hydrogen; development of hydrogen powered vehicles; and ''transformational technology'' related to production, storage, distribution, or use of hydrogen fuel. And importantly, the cash prizes would only go to individuals who produce breakthrough results in these categories, spurring competition and innovation into much needed technology.

Solution to our energy crisis can be found in our backyard. Hydrogen can be produced here on American soil. Companies such as UTC Power and Fuel Cell Energy in my district in Connecticut produce hydrogen fuel cells which are a clean, reliable form of energy. Technology such as this can relieve us from our dependence on foreign nations for our energy and create a much healthier alternative for our environment.

Mr. Speaker, I urge my colleagues to join me today in advancing science and supporting H.R. 632. It's time for us to take leadership and commit to the safety and health of our nation by inspiring our nation's brightest to make hydrogen technology a reality.

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

The SPEAKER pro tempore (Mr. SALAZAR). The question is on the motion offered by the gentleman from Illinois (Mr. LIPINSKI) that the House suspend the rules and pass the bill, H.R. 632, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

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

The yeas and nays were ordered.

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

SECURELY PROTECT YOURSELF AGAINST CYBER TRESPASS ACT

Mr. RUSH. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 964) 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 the title of the bill.

The text of the bill is as follows:

H.R. 964

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Securely Protect Yourself Against Cyber Trespass Act'' or the ''Spy Act''.

SEC. 2. PROHIBITION OF UNFAIR OR DECEPTIVE ACTS OR PRACTICES RELATING TO SPYWARE.

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

(1) Taking control of the computer by—

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

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

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

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

(C) accessing, hijacking, or otherwise using the modem, or Internet connection or service, for the computer and thereby causing damage to the computer or causing the owner or authorized user or a third party defrauded by such conduct to incur charges or other costs for a service that is not authorized by such owner or authorized user;

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

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

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

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

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

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

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

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

(4) Inducing the owner or authorized user of the computer to disclose personally identifiable information by means of a Web page that—

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

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

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

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

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

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

(7) Inducing the owner or authorized user to install or execute computer software by misrepresenting the identity or authority of the person or entity providing the computer software to the owner or user.

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

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

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

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

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

(b) GUIDANCE.—The Commission shall issue guidance regarding compliance with and violations of this section. This subsection shall take effect upon the date of the enactment of this Act.

(c) EFFECTIVE DATE.—Except as provided in subsection (b), this section shall take effect upon the expiration of the 6-month period that begins on the date of the enactment of this Act.

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

(a) OPT-IN REQUIREMENT.—Except as provided in subsection (e), it is unlawful for any person—

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

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

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

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

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

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

(b) INFORMATION COLLECTION PROGRAM.—

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

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

(i) collects personally identifiable information; and

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

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

(B) COLLECTION OF INFORMATION REGARDING INTERNET ACTIVITY TO DELIVER ADVERTISING.—The computer software—

(i) collects information regarding the user's Internet activity using the computer; and

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

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

(A) the only information collected by the software regarding the user's internet activity, and used to deliver advertising to, or display advertising on, the protected computer, is—

(i) information regarding Web pages within a particular Web site; or

(ii) in the case of any Internet-based search function, user-supplied search terms necessary to complete the search and return results to the user;

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

(i) the provider of the Web site accessed or Internet-based search function; or

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

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

(c) NOTICE AND CONSENT.—

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

(A) The notice clearly distinguishes a statement required under subparagraph (B) from any other information visually presented contemporaneously on the computer.

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

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

(ii) With respect to an information collection program described in subsection (b)(1)(B): ''This program will collect information about Web pages you access and will use that information to display advertising on your computer. Do you accept?''.

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

(C) The notice provides for the user—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(d) REQUIRED FUNCTIONS.—The functions required under this subsection to be included in an information collection program that executes any information collection functions with respect to a protected computer are as follows:

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

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

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

(2) IDENTITY FUNCTION.—

(A) IN GENERAL.—With respect only to an information collection program that uses information collected in the manner described in subparagraph (A)(ii)(II) or (B)(ii) of subsection (b)(1) and subject to subparagraph (B) of this paragraph, a function of the program

that provides that each display of an advertisement directed or displayed using such information, when the owner or authorized user is accessing a Web page or online location other than of the provider of the computer software, is accompanied by the name of the information collection program, a logogram or trademark used for the exclusive purpose of identifying the program, or a statement or other information sufficient to clearly identify the program.

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

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

(e) LIMITATION ON LIABILITY.—A telecommunications carrier, a provider of information service or interactive computer service, a cable operator, or a provider of transmission capability shall not be liable under this section to the extent that the carrier, operator, or provider—

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

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

(f) STUDY AND ADDITIONAL EXEMPTION.—

(1) STUDY AND REPORT.—The Commission shall conduct a study to determine the applicability of the information collection prohibitions of this section to information that is input directly by users in a field provided on a website. The study shall examine—

(A) the nature of such fields for user input;

(B) the use of a user's information once input and whether such information is sent to a person other than the provider of the Web site;

(C) whether such information is used to deliver advertisements to the user's computer; and

(D) the extent of any notice provided to the user prior to such input.

(2) REPORT.—The Commission shall transmit a report on such study to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate not later than the expiration of the 6-month period that begins on the date on which final regulations are issued under section 9. The requirements of subchapter I of chapter 35 of title 44, United States Code, shall not apply to the report required under this subsection.

(3) REGULATION.—If the Commission finds that users have adequate notice regarding the uses of any information input directly by the user in a field provided on a website, such that an exemption from the requirements of this section, or a modification of the notice required by this section is appropriate for such information, and that such an exemption or modification is consistent with the public interest, the protection of consumers, and the purposes of this Act, the Commission may prescribe such an exemption or modification by regulation.

SEC. 4. ENFORCEMENT.

(a) UNFAIR OR DECEPTIVE ACT OR PRACTICE.—This Act shall be enforced by the Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.). A violation of any provision of this Act or of a regulation issued under this Act shall be treated as an unfair or deceptive act or practice violating a rule promulgated under section 18 of the Federal Trade Commission Act (15 U.S.C. 57a).

(b) PENALTY FOR PATTERN OR PRACTICE VIOLATIONS.—

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

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

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

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

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

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

(c) REQUIRED SCIENTER.—Civil penalties sought under this section for any action may not be granted by the Commission or any court unless the Commission or court, respectively, establishes that the action was committed with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive or violates this Act.

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

(e) EXCLUSIVENESS OF REMEDIES.—The remedies in this section (and other remedies available to the Commission in an enforcement action against unfair and deceptive acts and practices) are the exclusive remedies for violations of this Act.

(f) EFFECTIVE DATE.—To the extent only that this section applies to violations of section 2(a), this section shall take effect upon the expiration of the 6-month period that begins on the date of the enactment of this Act.

SEC. 5. LIMITATIONS.

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

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

(2) the transmission or execution of an information collection program in compliance with a law enforcement, investigatory, national security, or regulatory agency or department of the United States or any State in response to a request or demand made under authority granted to that agency or department, including a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a court order, or other lawful process.

(b) EXCEPTION RELATING TO SECURITY.—Nothing in this Act shall apply to—

(1) any monitoring of, or interaction with, a protected computer—

(A) in connection with the provision of a network access service or other service or product with respect to which the user of the protected computer is an actual or prospective customer, subscriber, registered user, or account holder;

(B) by the provider of that service or product or with such provider's authorization; and

(C) that involves or enables the collection of information about the user's activities only with respect to the user's relationship with or use of such service or product,

to the extent that such monitoring or interaction is for the purpose of network security, computer security, diagnostics, technical support or repair, network management, authorized updates of software, 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.—

(1) IN GENERAL.—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.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed to limit the liability of a provider of computer software or of an interactive computer service for any anticompetitive act otherwise prohibited by law.

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

(e) SERVICES PROVIDED BY CABLE OPERATORS AND SATELLITE CARRIERS.—It shall not be a violation of section 3 for a satellite carrier (as such term is defined in section 338(k) of the Communications Act of 1934 (47 U.S.C. 338(k)) or cable operator (as such term is defined in section 631(a)(2) of such Act (47 U.S.C. 551(a)(2))) to—

(1) utilize a navigation device (as such term is defined in the rules of the Federal Communications Commission);

(2) interact with such a navigation device; or

(3) transmit software to or execute software installed on such a navigation device to provide service or collect or disclose subscriber information,

if the provision of such service, the utilization of or the interaction with such device, or the collection of or disclosure of such information, is subject to section 338(i) or section 631 of the Communications Act of 1934.

SEC. 6. EFFECT ON OTHER LAWS.

(a) PREEMPTION OF STATE LAW.—

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

(A) unfair or deceptive conduct with respect to computers similar to that described in section 2(a);

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

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

(2) ADDITIONAL PREEMPTION.—

(A) IN GENERAL.—No person other than the Attorney General of a State may bring a civil action under the law of any State if

such action is premised in whole or in part upon the defendant violating any provision of this Act.

(B) PROTECTION OF CONSUMER PROTECTION LAWS.—This paragraph shall not be construed to limit the enforcement of any State consumer protection law by an Attorney General of a State.

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

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

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

(4) EFFECTIVE DATE.—The preemption provided for under this subsection shall take effect, with respect to specific provisions of this Act, on the effective date for such provisions.

(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. FTC REPORT ON COOKIES.

(a) IN GENERAL.—Not later than the expiration of the 6-month period that begins on the date on which final regulations are issued under section 9, the Commission shall submit a report to the Congress regarding the use of cookies in the delivery or display of advertising to the owners and users of computers. The report shall examine the extent to which cookies are or may be used to transmit to a third party personally identifiable information of a computer owner or user, information regarding Web pages accessed by the owner or user, or information regarding advertisements previously delivered to a computer, for the purpose of—

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

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

The report shall examine and describe the methods by which cookies and the Web sites that place them on computers function separately and together, and shall compare the use of cookies with the use of information collection programs (as such term is defined in section 3) to determine the extent to which such uses are similar or different. The report may include such recommendations as the Commission considers necessary and appropriate, including treatment of cookies under this Act or other laws.

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

(c) PAPERWORK REDUCTION REQUIREMENTS.—The requirements of subchapter I of chapter 35 of title 44, United States Code, shall not apply to the report required under this section.

SEC. 8. FTC REPORT ON INFORMATION COLLECTION PROGRAMS INSTALLED BEFORE EFFECTIVE DATE.

Not later than the expiration of the 6-month period that begins on the date on which final regulations are issued under section 9, the Commission shall submit a report to the Congress on the extent to which there are installed on protected computers information collection programs that, but for installation prior to the effective date under section 11(a), would be subject to the requirements of section 3. The report shall include recommendations regarding the means of affording computer users affected by such information collection programs the protections of section 3, including recommendations regarding requiring a one-time notice and consent by the owner or authorized user of a computer to the continued collection of information by such a program so installed on the computer. The requirements of subchapter I of chapter 35 of title 44, United States Code, shall not apply to the report required under this section.

SEC. 9. REGULATIONS.

(a) IN GENERAL.—The Commission shall issue the regulations required by this Act not later than the expiration of the 9-month period beginning on the date of the enactment of this Act. In exercising its authority to issue any regulation under this Act, the Commission shall determine that the regulation is consistent with the public interest and the purposes of this Act. Any regulations issued pursuant to this Act shall be issued in accordance with section 553 of title 5, United States Code.

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

SEC. 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(b)(1)(A), does not include obtaining of the information by a party who is intended by the owner or authorized user of a protected computer to receive the information or by a third party authorized by such intended recipient to receive the information, pursuant to the owner or authorized user—

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

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

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

(4) COMPUTER SOFTWARE.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''computer 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) EXCEPTIONS.—Such term does not include—

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

(ii) a cookie; or

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

(5) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(6) DAMAGE.—The term ''damage'' has the meaning given such term in section 1030(e) of title 18, United States Code.

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

(8) DISABLE.—The term ''disable'' means, with respect to an information collection program, to permanently prevent such program from executing any of the functions described in section 3(b)(1) that such program is otherwise capable of executing (including by removing, deleting, or disabling the program), unless the owner or operator of a protected computer takes a subsequent affirmative action to enable the execution of such functions.

(9) INFORMATION COLLECTION FUNCTIONS.—The term ''information collection functions'' means, with respect to an information collection program, the functions of the program described in subsection (b)(1) of section 3.

(10) INFORMATION SERVICE.—The term ''information service'' has the meaning given such term in section 3 of the Communications Act of 1934 (47 U.S.C. 153).

(11) INTERACTIVE COMPUTER SERVICE.—The term ''interactive computer service'' has the meaning given such term in section 230(f) of the Communications Act of 1934 (47 U.S.C. 230(f)).

(12) INTERNET.—The term ''Internet'' means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio.

(13) PERSONALLY IDENTIFIABLE INFORMATION.—

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

(i) First and last name of an individual.

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

(iii) An electronic mail address.

(iv) A telephone number.

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

(vi) A credit card number.

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

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

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

(14) SUITE OF FUNCTIONALLY RELATED SOFTWARE.—The term suite of ''functionally related software'' means a group of computer software programs distributed to an end user by a single provider, which programs enable features or functionalities of an integrated service offered by the provider.

(15) TELECOMMUNICATIONS CARRIER.—The term ''telecommunications carrier'' has the meaning given such term in section 3 of the Communications Act of 1934 (47 U.S.C. 153).

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

(17) WEB PAGE.—The term ''Web page'' means a location, with respect to the World

Wide Web, that has a single Uniform Resource Locator or another single location with respect to the Internet, as the Federal Trade Commission may prescribe.

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

(A) A common domain name.

(B) Common ownership, management, or registration.

SEC. 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, 2013.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Illinois (Mr. RUSH) and the gentleman from Florida (Mr. STEARNS) each will control 20 minutes.

The Chair recognizes the gentleman from Illinois.

GENERAL LEAVE

Mr. RUSH. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and to include extraneous material on the bill under consideration.

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

There was no objection.

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

Mr. Speaker, today the House takes up H.R. 964, the Securely Protect Yourself Against Cyber Trespass Act, or SPY Act.

This bill is not unfamiliar to the House of Representatives. Twice this body has passed the SPY Act with overwhelming margins, and it is my hope that today will be the third time. H.R. 964 aggressively tackles the problem of ''spyware,'' the insidious software that consumers unwittingly download onto their computers, only to have their personal private information extracted for commercial or fraudulent purposes.

In the past two Congresses, Mrs. BONO and Mr. TOWNS introduced the bipartisan SPY Act, and both times the bill enjoyed overwhelming support. This year, Mr. TOWNS and Mrs. BONO have once again teamed up to introduce the SPY Act as H.R. 964. And on March 15, the Consumer Protection Subcommittee held another legislative hearing on the bill. On May 10, 2007, the Energy and Commerce Committee unanimously reported H.R. 964, the SPY Act, as amended.

H.R. 964 provides a broad regulatory framework that empowers consumers with knowledge and the ability to control what software is installed, and is not installed, on their personal computers. This bill prohibits unfair or deceptive acts and practices related to spyware and creates an ''opt in'' regime whereby entity cannot execute any program that collects a person's personal information without, first, giving explicit notice to the consumer and second, receiving his or her consent. H.R. 964 provides that the FTC will enforce the SPY Act and will have the authority to impose significant civil penalties. During both the full committee and the subcommittee markups of H.R. 964, I introduced manager's amendments tweaking provisions of the bill, and they were the work product of deliberative bipartisan cooperation. This bill has been thoroughly honed to be effective without being overbearing.

Mr. Speaker, the SPY Act is a quality piece of legislation that all Members of the House should enthusiastically support. The full Committee on Energy and Commerce and the subcommittee that I am privileged to chair, the Subcommittee on Commerce, Trade and Consumer Protection, have a long history of bipartisan cooperation, and this bill is an extension of that longstanding tradition.

I urge my colleagues to vote ''yes'' on the bill.

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

Mr. STEARNS. Mr. Speaker, I yield myself such time as I may consume. Mr. Speaker, I am pleased again, I have been here a number of times, to consider H.R. 964, the SPY Act, a bill which is important to fight Internet privacy. In the past and as we speak on the floor today, this has bipartisan support with bipartisan leadership. It has been offered by my colleague from California, MARY BONO, and my colleague from New York, ED TOWNS. Both of them have worked dutifully to try to pass this bill. And, unfortunately, the last time we passed it overwhelmingly in the House, it did not get through the Senate; so we are back at it again.

I also want to thank the new chairman of the committee that I chaired last year, Mr. RUSH, for his commitment to maintaining a bipartisan process in this, and that is why we are here on the floor today. If it hadn't been for the leadership of these individuals combined with what I think is a Federal Trade Commission commitment and the stakeholders in the community in this process, we would not have had a workable legislative solution.

So I think today that we have to realize that even at the last 11th hour we might have some people who don't totally agree, but I think the bill is a strong bill. It takes a firm and, I think, a fair on balance approach in balancing the need to address bad actors and the need to protect the functions of legitimate business tools.

Both at the committee level and on the floor, we have voted on this spyware before, as I mentioned, three times. Three times we have gone through the process of holding hearings, receiving testimony from many witnesses, listening to the horrors of spyware and how it can be a tool of identity thieves, and we know how identity theft is prevalent today, conducting negotiations, and we have asked for ways to improve the bill. So we have seen support across the board in industry for this bill. We asked what is the best way to improve this bill. So I think we have worked hard on this legislation.

And, my colleagues, I think it is time we move this to the Senate, and if there are any further problems with this bill, we certainly can handle these problems in the conference between the House and the Senate.

Now, you should realize that there are some in the business community who have raised a 11th hour concern about a specific provision that was added at the full committee markup. Not in our subcommittee, Mr. Speaker, but in our full committee. I have been through seven hearings on the question of privacy on the question of opt in and opt out. I am well aware of the feelings of Members dealing with opt in and opt out, depending upon how you view this process. So I share some of the concerns of the business community in their 11th hour attempt to bring this to our attention. But the responsibility of continuing to move this process forward, I think, is important. That is why I have decided to vote ''yes'' today to support this bill. And, hopefully, when the Senate has it, they can make the changes. If not, we can do it in conference. But to take a bill that has been in this long process and has had so many hearings for so many years and decide that it should not go forward is not the right process.

□ 1220

And we all in Congress here know that sometimes the enemy of the good is the perfect.

So we can solve this issue, I think, to satisfy all interested parties. It is a strong piece of legislation; and I cannot think of a reason why our Senate colleagues should not act on it, also.

So, in closing, the SPY Act is a solid consumer protection bill that returns control of personal computers and private information to where it belongs, and that is to the consumer.

I urge my colleagues to vote ''yes'' on H.R. 964.

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

Mr. RUSH. Mr. Speaker, I am pleased to yield 5 minutes to the gentleman from New York, my colleague, my friend (Mr. TOWNS).

Mr. TOWNS. Thank you very much for yielding time.

Mr. Speaker, I rise in support of H.R. 964, the SPY Act, which would greatly improve the privacy of consumers' online computer use. The time has come for this bill to pass.

A lot of hard work has been put into this legislation. First and foremost, I

would like to commend Congresswoman MARY BONO, the Republican sponsor of the bill. Of course, without her hard work, insight and persistence on this issue, we would not be where we are today. I have been proud to work with her on this bill, and I salute her for all of her efforts.

Of course, we have been down this road a few times now with several hearings; and, of course, we passed it before. But this time I think that people realize how important this legislation is, and I do feel that it should go all the way.

I also want to commend Chairman DINGELL and Ranking Member BARTON for their strong commitment to this issue and leadership in getting our bill to the floor. I would like to thank my very good friend, the subcommittee chairman, Chairman RUSH of Chicago, Illinois, Ranking Member STEARNS, who has been a friend for many, many years as well, for their hard work on this legislation. They have stayed with it and gone through the process over and over again because they recognize how important this legislation is to our country.

Finally, I would like to acknowledge all of the staff for their hard work, especially Consuela Washington and David Cavicke for their hard work and, of course, their suggestions and ideas and recommendations. I would like to just take this opportunity to thank them.

There is no question that spyware is a serious problem. Spyware software, which is downloaded without a computer owner's knowledge, invades one's privacy by recording and transmitting personal information, monitoring the Web site someone visits, or even stealing documents from an individual's computer. Other programs hijack a computer by changing home pages or forcing a person to click through multiple screens until a spyware program is downloaded.

In fact, problems related to spyware have become so widespread that I cannot run into someone who hasn't been negatively affected by it. This is a big change from when we first began this effort a few years ago. There were only a few people complaining, but now we have a lot of people complaining. Now we know the seriousness of the problem and that we need Federal legislation to safeguard privacy, as well as to ensure the long-term integrity of e-commerce.

Today's legislation provides consumers with new tools to protect themselves from unwanted, harmful software. 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, Mr. Speaker, consumers must have the option to easily disable any harmful spyware programs to their computer. While some consumers may want to share their information to receive free games other discount offers, all consumers have the right to make that choice.

Finally, Mr. Speaker, and this time I really mean finally, any time we legislate on highly technical matters there is always a danger of stifling innovation and 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 tightrope.

This bill addresses many of the concerns raised, while at the same time retaining a meaningful notice and consent regime to protect consumer privacy.

Through much hard work, we have carefully crafted a strong bipartisan consumer protection bill, and I would urge my colleagues to support this. This is a quality piece of legislation, and I hope that we are able to move it through both Houses very quickly and that the President would sign it into law.

Mr. STEARNS. Mr. Speaker, I yield 5 minutes to the author of the bill, the gentlelady from California (Mrs. BONO).

Mrs. BONO. Mr. Speaker, I rise in strong support of H.R. 964, the Securely Protect Yourself Against Cyber Trespass Act.

When the gentleman from New York and I first introduced the spyware bill in 2003, few people knew what spyware was or how problematic it could be to American citizens; and since that time the online threat of spyware remains. According to a recent Consumer Report survey, spyware and viruses cost American computer users nearly $8 billion over a 2-year period.

Historically, spyware legislation in this House has received strong bipartisan support. Our initial bill in the 108th Congress passed 399–1; and in the 109th Congress, our spyware bill again received overwhelming bipartisan support, garnering over 60 cosponsors and passing the House 393–4.

Mr. Speaker, this Congress, H.R. 964, the Securely Protect Yourself Against Cyber Trespass Act, or SPY Act, has again garnered wide bipartisan support with 41 cosponsors.

Because of the Internet's role in interstate commerce, the need for Federal spyware legislation is clear. We cannot expect online companies to function efficiently when they are faced with a patchwork of State anti-spyware statutes. There needs to be legal uniformity.

Additionally, I remain a strong proponent of anti-spyware legislation because I believe consumers should have the final say about what plants itself on their computer, not a third party with potentially conflicting interests. The SPY Act accomplishes this by prohibiting commonly known, unfair or deceptive acts relating to spyware.

H.R. 964 also prohibits the collection of personal information from a computer without notice and consent before the first execution of any information collection program. The bill also requires that the user is able to easily remove or disable the spyware.

I also understand there are instances where spyware can be useful. H.R. 964 exempts action taken by law enforcement and national security pursuant to warrant, court order or other lawful process, or actions taken in good faith with the user's consent. H.R. 964 also protects the developers of anti-spyware software from the threat of serious lawsuits.

Simply stated, this bill works to restore privacy on the home computer, which has become the control center for our business transactions as well as as our personal interactions.

Mr. Speaker, my colleague from New York and I began this effort in 2003; and I thank the gentleman, ED TOWNS, for all of his efforts and for being such a terrific partner in this process. Again, since that time, this effort has received the bipartisan support of the House. It is my hope that the 110th Congress will continue to act in a bipartisan way that passes this legislation.

I ask for the support of my colleagues and hope that once again we can take back our computers so the consumer owns their computer, not a third party. Let's pass the SPY Act, H.R. 984.

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

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

Mr. RUSH. Mr. Speaker, as was indicated earlier, this is the third time that this bill has been before this body. It was passed overwhelmingly two times in prior Congresses. We really believe that the third time should be the charm. This bill should pass out of this House with the same kind of margins that it passed out of two previous Congresses, and I would urge my colleagues to vote for this bill once again.

This bill needs to become law. This bill protects the American consumer. This bill protects the American economy. This is a good bill. It needs to become law.

None of the practices outlawed by section 2 of the bill are ''legitimate.'' As for section 3's consumer notice, consent, identification, and easy disabling requirements, legitimate business practices are exempted by the exceptions in section 3(b)(2) and the limitations in section 5 of the SPY Act. The committee added new rule-making authority to exempt a broad class of entities operating Internet Web sites that collect information if the FTC finds that their notice to consumers is adequate.

□ 1230

Mr. Speaker, we have corrected the bill, made minor tweaking improvements on the bill, and I urge my colleagues to support this bill.

Ms. SCHAKOWSKY. Mr. Speaker, I rise today in strong support of H.R. 964, the Securely Protect Yourself Against Cyber Trespass Act—the SPY Act. It is a strong consumer protection bill, of which I am an original cosponsor, that will help us in the fight against identity theft.

With today's vote, the House will have passed the SPY Act three times. Let's hope that the third time's a charm—and that today's passage means this bill will finally get signed into law.

The SPY Act is important because it protects consumers from spyware, the unwanted and sneaky software that is so powerful that it can steal information from, monitor and control others' computers—without the computer's owner even knowing the software has been installed.

The SPY Act would put the control of computers back in the hands of consumers—where it belongs. It prohibits indefensible uses of the software, like phishing and logging every keystroke entered, and requires that consumers be notified and opt-in before software is installed on their computers. Furthermore, the SPY Act gives the Federal Trade Commission the additional power it needs to pursue deceptive uses of the software.

I believe that this bill will go a long way toward protecting consumers from having their valuable and personal information stolen by purveyors of spyware. I am glad that I was part of the bipartisan process that brought this bill to the floor today. I urge my colleagues to support its passage. Thank you.

Mr. GOODLATTE. Mr. Speaker, I rise in opposition to H.R. 964, the SPY Act.

The continued growth of the Internet has brought tremendous enhancements to our quality of life—from advances in the delivery of health care, to the ability of consumers to instantaneously conduct transactions online. Increasingly, consumers want a fast connection to the Internet and want the delivery of online services to be seamless and online service providers have invested significant resources to develop software to make their services as safe, reliable and fast as possible.

However, as Congress considers legislation to combat spyware, I believe that four overarching principles should guide our efforts. First, we must punish the bad actors, while protecting legitimate online companies. Second, we must not over-regulate, but rather encourage innovative new services and the growth of the Internet. Third, we must not stifle the tree market interactions between consumers and service providers. Fourth, we must target the behavior, not the technology. It is my hope that any legislation Congress enacts to combat spyware will adhere to these core principles.

On May 23, 2005, the House of Representatives passed legislation, similar to H.R. 964, which sought to solve the spyware problem by targeting the technology, instead of the criminal behavior behind the technology. However, many developments have occurred during the intervening two years which have convinced me that this regulatory approach to combating spyware is even more unwise than previously thought.

For example, just last month, the House Energy and Commerce Committee adopted an amendment to H.R. 964 that would have had enormous consequences for the Internet and online innovation. This amendment would have, in part, regulated Internet ''cookies'' for the first time under the bill. Internet cookies are used by most websites to enhance consumers' experiences with the Internet and to make the Internet more seamless and navigable with fewer stoplights. To make every online company that uses cookies comply with the notice and consent regime under the bill would have significantly interfered with consumers' Internet experiences. By forcing consumers to click through even more prescripted alert messages, this change would have, ironically, exacerbated the likelihood that consumers would become desensitized to these notices and click ''accept'' without reading them. In addition, this desensitization is likely to also give nefarious software installers a false legitimacy since there would be no distinction between the notices they provide and the notices legitimate online companies provide.

Apparently, the Democratic Leadership saw the error in the regulation of cookies and stripped the bill of this language just before the bill came to the Floor today. However, this mistake by the committee highlights the difficulties with trying to impose one-size-fits-all regulations to solve problems involving ever-evolving technologies.

In addition, Chairman Majoras of the Federal Trade Commission testified in October of 2005 that a notice-and-choice approach was not recommended for combating spyware for many reasons. He noted the fact that consumers will be overwhelmed by the notices they will receive when using the Internet and will most likely ignore the notices and click through them.

Furthermore, in the past few years there have been major developments in technological solutions to help consumers combat spyware. Consumer packages are becoming more and more effective in screening out unwanted spyware from their computers and are offered by many Internet service providers, as well as independent software providers.

Finally, a broad cross-section of legitimate online businesses and trade associations has expressed opposition to the regulatory approach of H.R. 964. On June 5, 2007, a coalition of over 30 trade associations and companies, including the U.S. Chamber of Commerce, the National Retail Federation, the Financial Services Roundtable, and numerous technology-based entities, sent a letter to all Members of the House of Representatives detailing their concerns with H.R. 964. This letter specifically expresses opposition to regulating Internet cookies, as well as opposition to including web sites (where consumers willingly submit information online) within in the scope of the legislation.

The better approach to combating spyware would be to target the criminal behavior of those who actually use spyware, and to continue our policy of letting innovative online companies interact with consumers to develop the exciting new online services that consumers have come to enjoy and expect from the Internet.

I have introduced legislation, along with my colleague ZOE LOFGREN of California, to combat spyware by going after the criminals using spyware, rather than trying to regulate all software regardless of whether it is harmful or helpful. This legislation, H.R. 1525, was passed by the House and now awaits further action in the Senate. I urge my colleagues to support this targeted approach.

Mr. BARTON of Texas. Mr. Speaker, the bill we are considering today—the Towns-Bono SPY Act—is an important piece of legislation to me. We've been working on this bill for 4 years now, before many of us ever heard the term ''spyware.'' I applaud the bipartisan sponsors for their unwavering commitment to pass this legislation.

The surreptitious installation of spyware on your computer without your knowledge and without your consent is a little like sneaking into your home and planting a bug: it is an invasion of your privacy and it is clearly wrong. This bill prohibits all the nefarious conduct that is used to harm consumers. The legislation provides the FTC a strong mandate to go after bad actors and their destructive behavior.

There are many important and legitimate business functions of the Internet, and I have no problem with businesses trying to compete and sell their goods and services. And I recognize advertising is a part of commerce. But I feel strongly that there is a line that should not be crossed regarding the sharing of my personal information without first obtaining my consent. Consumers have the right to know if they are being profiled, if their personal information is going to be shared, and with whom it might be shared. My computer and my personal information are my property. This legislation will ensure I have control over both.

This bill strikes a fair balance between the need to protect the functions of legitimate business tools and punishing bad actors.

In closing, I want to thank Chairman RUSH, Chairman DINGELL, and Ranking Member STEARNS for moving the bill through the Committee. I commend MARY BONO and ED TOWNS for their tireless efforts to address this insidious activity.

I urge all of my colleagues to vote for this important piece of legislation and hope that our Senate colleagues will do the same.

Mr. RUSH. 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 Illinois (Mr. RUSH) that the House suspend the rules and pass the bill, H.R. 964, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

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

The yeas and nays were ordered.

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

HUMAN CLONING PROHIBITION ACT OF 2007

Ms. DEGETTE. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2560) to amend the Federal Food, Drug, and Cosmetic Act to prohibit human cloning, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 2560

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 ''Human Cloning Prohibition Act of 2007''.

SEC. 2. PROHIBITION AGAINST HUMAN CLONING.

(a) IN GENERAL.—The Federal Food, Drug, and Cosmetic Act (21 U.S.C. 301 et seq.) is amended by adding at the end the following: