

HEINONLINE

Citation: 1 Controlling the Assault of Non-Solicited Pornography
Marketing CAN-SPAM Act of 2003 A Legislative History
H. Manz ed. 2186 2004

Content downloaded/printed from
HeinOnline (<http://heinonline.org>)
Mon Apr 22 11:18:06 2013

- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at <http://heinonline.org/HOL/License>
- The search text of this PDF is generated from uncorrected OCR text.

Mr. LINDER. Mr. Speaker, I yield back the balance of my time, and I move the previous question on the resolution.

The SPEAKER pro tempore. The question is on ordering the previous question.

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

Mr. FROST. 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, further proceedings on this motion will be postponed.

A FURTHER MESSAGE FROM THE SENATE

A further message from the Senate by Mr. Monahan, one of its clerks, announced that the Senate agrees to the report of the committee of conference on the disagreeing votes of the two Houses on the amendment of the Senate to the bill (H.R. 1904) "An Act to improve the capacity of the Secretary of Agriculture and the Secretary of the Interior to plan and conduct hazardous fuels reduction projects on National Forest System lands and Bureau of Land Management lands aimed at protecting communities, watersheds, and certain other at-risk lands from catastrophic wildfire, to enhance efforts to protect watersheds and address threats to forest and rangeland health, including catastrophic wildfire, across the landscape, and for other purposes."

CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING ACT OF 2003

Mr. TAUZIN. Mr. Speaker, I move to suspend the rules and pass the Senate bill (S. 877) to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet, as amended.

The Clerk read as follows:

S. 877

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 "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003", or the "CAN-SPAM Act of 2003".

SEC. 2. CONGRESSIONAL FINDINGS AND POLICY.

(a) FINDINGS.—The Congress finds the following:

(1) Electronic mail has become an extremely important and popular means of communication, relied on by millions of Americans on a daily basis for personal and commercial purposes. Its low cost and global reach make it extremely convenient and efficient, and offer unique opportunities for the development and growth of frictionless commerce.

(2) The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail. Unsolicited

commercial electronic mail is currently estimated to account for over half of all electronic mail traffic, up from an estimated 7 percent in 2001, and the volume continues to rise. Most of these messages are fraudulent or deceptive in one or more respects.

(3) The receipt of unsolicited commercial electronic mail may result in costs to recipients who cannot refuse to accept such mail and who incur costs for the storage of such mail, or for the time spent accessing, reviewing, and discarding such mail, or for both.

(4) The receipt of a large number of unwanted messages also decreases the convenience of electronic mail and creates a risk that wanted electronic mail messages, both commercial and noncommercial, will be lost, overlooked, or discarded amidst the larger volume of unwanted messages, thus reducing the reliability and usefulness of electronic mail to the recipient.

(5) Some commercial electronic mail contains material that many recipients may consider vulgar or pornographic in nature.

(6) The growth in unsolicited commercial electronic mail imposes significant monetary costs on providers of Internet access services, businesses, and educational and nonprofit institutions that carry and receive such mail, as there is a finite volume of mail that such providers, businesses, and institutions can handle without further investment in infrastructure.

(7) Many senders of unsolicited commercial electronic mail purposefully disguise the source of such mail.

(8) Many senders of unsolicited commercial electronic mail purposefully include misleading information in the message's subject lines in order to induce the recipients to view the messages.

(9) While some senders of commercial electronic mail messages provide simple and reliable ways for recipients to reject (or "opt-out" of) receipt of commercial electronic mail from such senders in the future, other senders provide no such "opt-out" mechanism, or refuse to honor the requests of recipients not to receive electronic mail from such senders in the future, or both.

(10) Many senders of bulk unsolicited commercial electronic mail use computer programs to gather large numbers of electronic mail addresses on an automated basis from Internet websites or online services where users must post their addresses in order to make full use of the website or service.

(11) Many States have enacted legislation intended to regulate or reduce unsolicited commercial electronic mail, but these statutes impose different standards and requirements. As a result, they do not appear to have been successful in addressing the problems associated with unsolicited commercial electronic mail. In part because, since an electronic mail address does not specify a geographic location, it can be extremely difficult for law-abiding businesses to know with which of these disparate statutes they are required to comply.

(12) The problems associated with the rapid growth and abuse of unsolicited commercial electronic mail cannot be solved by Federal legislation alone. The development and adoption of technological approaches and the pursuit of cooperative efforts with other countries will be necessary as well.

(b) CONGRESSIONAL DETERMINATION OF PUBLIC POLICY.—On the basis of the findings in subsection (a), the Congress determines that—

(1) there is a substantial government interest in regulation of commercial electronic mail on a nationwide basis;

(2) senders of commercial electronic mail should not mislead recipients as to the source or content of such mail; and

(3) recipients of commercial electronic mail have a right to decline to receive additional commercial electronic mail from the same source.

SEC. 3. DEFINITIONS.

In this Act:

(1) AFFIRMATIVE CONSENT.—The term "affirmative consent", when used with respect to a commercial electronic mail message, means that—

(A) the recipient expressly consented to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient's own initiative; and

(B) if the message is from a party other than the party to which the recipient communicated such consent, the recipient was given clear and conspicuous notice at the time the consent was communicated that the recipient's electronic mail address could be transferred to such other party for the purpose of initiating commercial electronic mail messages.

(2) COMMERCIAL ELECTRONIC MAIL MESSAGE.—

(A) IN GENERAL.—The term "commercial electronic mail message" means any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose).

(B) TRANSACTIONAL OR RELATIONSHIP MESSAGES.—The term "commercial electronic mail message" does not include a transactional or relationship message.

(C) REGULATIONS REGARDING PRIMARY PURPOSE.—Not later than 12 months after the date of the enactment of this Act, the Commission shall issue regulations pursuant to section 13 further defining the relevant criteria to facilitate the determination of the primary purpose of an electronic mail message.

(D) REFERENCE TO COMPANY OR WEBSITE.—The inclusion of a reference to a commercial entity or a link to the website of a commercial entity in an electronic mail message does not, by itself, cause such message to be treated as a commercial electronic mail message for purposes of this Act if the contents or circumstances of the message indicate a primary purpose other than commercial advertisement or promotion of a commercial product or service.

(3) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(4) DOMAIN NAME.—The term "domain name" means any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.

(5) ELECTRONIC MAIL ADDRESS.—The term "electronic mail address" means a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the "local part") and a reference to an Internet domain (commonly referred to as the "domain part"), whether or not displayed, to which an electronic mail message can be sent or delivered.

(6) ELECTRONIC MAIL MESSAGE.—The term "electronic mail message" means a message sent to a unique electronic mail address.

(7) FTC ACT.—The term "FTC Act" means the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(8) HEADER INFORMATION.—The term "header information" means the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or

purporting to identify, a person initiating the message.

(9) **INITIATE.**—The term “initiate”, when used with respect to a commercial electronic mail message, means to originate or transmit such message or to procure the origination or transmission of such message, but shall not include actions that constitute routine conveyance of such message. For purposes of this paragraph, more than 1 person may be considered to have initiated a message.

(10) **INTERNET.**—The term “Internet” has the meaning given that term in the Internet Tax Freedom Act (47 U.S.C. 151 nt).

(11) **INTERNET ACCESS SERVICE.**—The term “Internet access service” has the meaning given that term in section 231(e)(4) of the Communications Act of 1934 (47 U.S.C. 231(e)(4)).

(12) **PROCURE.**—The term “procure”, when used with respect to the initiation of a commercial electronic mail message, means intentionally to pay or provide other consideration to, or induce, another person to initiate such a message on one’s behalf.

(13) **PROTECTED COMPUTER.**—The term “protected computer” has the meaning given that term in section 1030(e)(2)(B) of title 18, United States Code.

(14) **RECIPIENT.**—The term “recipient”, when used with respect to a commercial electronic mail message, means an authorized user of the electronic mail address to which the message was sent or delivered. If a recipient of a commercial electronic mail message has 1 or more electronic mail addresses in addition to the address to which the message was sent or delivered, the recipient shall be treated as a separate recipient with respect to each such address. If an electronic mail address is reassigned to a new user, the new user shall not be treated as a recipient of any commercial electronic mail message sent or delivered to that address before it was reassigned.

(15) **ROUTINE CONVEYANCE.**—The term “routine conveyance” means the transmission, routing, relaying, handling, or storing, through an automatic technical process, of an electronic mail message for which another person has identified the recipients or provided the recipient addresses.

(16) **SENDER.**—

(A) **IN GENERAL.**—Except as provided in subparagraph (B), the term “sender” means a person who initiates such a message and whose product, service, or Internet web site is advertised or promoted by the message.

(B) **SEPARATE LINES OF BUSINESS OR DIVISIONS.**—If an entity operates through separate lines of business or divisions and holds itself out to the recipient of the message, in complying with the requirement under section 5(a)(5)(B), as that particular line of business or division rather than as the entity of which such line of business or division is a part, then the line of business or the division shall be treated as the sender of such message for purposes of this Act.

(17) **TRANSACTIONAL OR RELATIONSHIP MESSAGE.**—

(A) **IN GENERAL.**—The term “transactional or relationship message” means an electronic mail message the primary purpose of which is—

(i) to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender;

(ii) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient;

(iii) to provide—

(I) notification concerning a change in the terms or features of;

(II) notification of a change in the recipient’s standing or status with respect to; or

(III) at regular periodic intervals, account balance information or other type of account statement with respect to,

a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender;

(iv) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or

(v) to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.

(B) **MODIFICATION OF DEFINITION.**—The Commission by regulation pursuant to section 13 may modify the definition in subparagraph (A) to expand or contract the categories of messages that are treated as transactional or relationship messages for purposes of this Act to the extent that such modification is necessary to accommodate changes in electronic mail technology or practices and accomplish the purposes of this Act.

SEC. 4. PROHIBITION AGAINST PREDATORY AND ABUSIVE COMMERCIAL E-MAIL.

(a) **OFFENSE.**—

(1) **IN GENERAL.**—Chapter 47 of title 18, United States Code, is amended by adding at the end the following new section:

“§ 1037. Fraud and related activity in connection with electronic mail

“(a) **IN GENERAL.**—Whoever, in or affecting interstate or foreign commerce, knowingly—

“(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,

“(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,

“(3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,

“(4) registers, using information that materially falsifies the identity of the actual registrant, for 5 or more electronic mail accounts or online user accounts or 2 or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or

“(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses,

or conspires to do so, shall be punished as provided in subsection (b).

“(b) **PENALTIES.**—The punishment for an offense under subsection (a) is—

“(1) a fine under this title, imprisonment for not more than 5 years, or both, if—

“(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or

“(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;

“(2) a fine under this title, imprisonment for not more than 3 years, or both, if—

“(A) the offense is an offense under subsection (a)(1);

“(B) the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations;

“(C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period;

“(D) the offense caused loss to 1 or more persons aggregating \$5,000 or more in value during any 1-year period;

“(E) as a result of the offense any individual committing the offense obtained anything of value aggregating \$5,000 or more during any 1-year period; or

“(F) the offense was undertaken by the defendant in concert with 3 or more other persons with respect to whom the defendant occupied a position of organizer or leader; and

“(3) a fine under this title or imprisonment for not more than 1 year, or both, in any other case.

“(c) **FORFEITURE.**—

“(1) **IN GENERAL.**—The court, in imposing sentence on a person who is convicted of an offense under this section, shall order that the defendant forfeit to the United States—

“(A) any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and

“(B) any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offense.

“(2) **PROCEDURES.**—The procedures set forth in section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) of that section, and in Rule 32.2 of the Federal Rules of Criminal Procedure, shall apply to all stages of a criminal forfeiture proceeding under this section.

“(d) **DEFINITIONS.**—In this section:

“(1) **LOSS.**—The term “loss” has the meaning given that term in section 1030(e) of this title.

“(2) **MATERIALLY.**—For purposes of paragraphs (3) and (4) of subsection (a), header information or registration information is materially misleading if it is altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation.

“(3) **MULTIPLE.**—The term “multiple” means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period.

“(4) **OTHER TERMS.**—Any other term has the meaning given that term by section 3 of the CAN-SPAM Act of 2003.”

(2) **CONFORMING AMENDMENT.**—The chapter analysis for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

“Sec.

“1037. Fraud and related activity in connection with electronic mail.”

(B) **UNITED STATES SENTENCING COMMISSION.**—

(1) **DIRECTIVE.**—Pursuant to its authority under section 984(p) of title 28, United States Code, and in accordance with this section, the United States Sentencing Commission shall review and, as appropriate, amend the sentencing guidelines and policy statements to provide appropriate penalties for violations of section 1037 of title 18, United States Code, as added by this section, and other offenses that may be facilitated by the sending

of large quantities of unsolicited electronic mail.

(2) **REQUIREMENTS.**— In carrying out this subsection, the Sentencing Commission shall consider providing sentencing enhancements for—

(A) those convicted under section 1037 of title 18, United States Code, who—
(i) obtained electronic mail addresses through improper means, including—

(I) harvesting electronic mail addresses of the users of a website, proprietary service, or other online public forum operated by another person, without the authorization of such person; and
(II) randomly generating electronic mail addresses by computer; or

(i) knew that the commercial electronic mail messages involved in the offense contained or advertised an Internet domain for which the registrant of the domain had provided false registration information; and
(B) those convicted of other offenses, including offenses involving fraud, identity theft, obscenity, child pornography, and the sexual exploitation of children, if such offenses involved the sending of large quantities of electronic mail.

(c) **SENSE OF CONGRESS.**— It is the sense of Congress that—
(1) Spam has become the method of choice for those who distribute pornography, perpetrate fraudulent schemes, and introduce viruses, worms, and Trojan horses into personal and business computer systems; and
(2) the Department of Justice should use all existing law enforcement tools to investigate and prosecute those who send bulk commercial e-mail to facilitate the commission of Federal crimes, including the tools contained in chapters 47 and 63 of title 18, United States Code (relating to fraud and false statements); chapter 71 of title 18, United States Code (relating to obscenity); chapter 110 of title 18, United States Code (relating to the sexual exploitation of children); and chapter 95 of title 18, United States Code (relating to racketeering); and appropriate.

SEC. 5. OTHER PROTECTIONS FOR USERS OF COMMERCIAL ELECTRONIC MAIL.

(a) **REQUIREMENTS FOR TRANSMISSION OF MESSAGES.**—
(1) **PROHIBITION OF FALSE OR MISLEADING TRANSMISSION INFORMATION.**— It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading. For purposes of this paragraph—
(A) header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading;
(B) a "from" line (the line identifying or purporting to identify a person initiating the message) that accurately identifies any person who initiated the message shall not be considered materially false or materially misleading; and
(C) header information shall be considered materially misleading if it fails to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin.

(2) **PROHIBITION OF DECEPTIVE SUBJECT HEADINGS.**— It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail mes-

sage if such person has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message (consistent with the criteria are used in enforcement of section 5 of the Federal Trade Commission Act (15 U.S.C. 45)).

(3) **INCLUSION OF RETURN ADDRESS OR COMPARABLE MECHANISM IN COMMERCIAL ELECTRONIC MAIL.**—

(A) **IN GENERAL.**— It is unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message that does not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that—
(i) a recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received; and
(ii) remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message.

(B) **MORE DETAILED OPTIONS POSSIBLE.**— The person initiating a commercial electronic mail message may comply with subparagraph (A)(i) by providing the recipient a list or menu from which the recipient may choose the specific types of commercial electronic mail messages the recipient wants to receive or does not want to receive from the sender, if the list or menu includes an option under which the recipient may choose not to receive any commercial electronic mail messages from the sender.

(C) **TEMPORARY INABILITY TO RECEIVE MESSAGES OR PROCESS REQUESTS.**— A return electronic mail address or other mechanism does not fail to satisfy the requirements of subparagraph (A) if it is unexpectedly and temporarily unable to receive messages or process requests due to a technical problem beyond the control of the sender if the problem is corrected within a reasonable time period.

(4) **PROHIBITION OF TRANSMISSION OF COMMERCIAL ELECTRONIC MAIL AFTER OBJECTION.**—
(A) **IN GENERAL.**— If a recipient makes a request using a mechanism provided pursuant to paragraph (3) not to receive some or any commercial electronic mail messages from such sender, then it is unlawful—
(i) for the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message that falls within the scope of the request;
(ii) for any person acting on behalf of the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message falls within the scope of the request;
(iii) for any person acting on behalf of the sender to assist in initiating the transmission to the recipient, through the provision or selection of addresses to which the message will be sent, of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message would violate clause (i) or (ii); or
(iv) for the sender, or any other person who knows that the recipient has made such a request, to sell, lease, exchange, or otherwise transfer or release the electronic mail address of the recipient (including through any transaction or other transfer involving mail-

ing lists bearing the electronic mail address of the recipient) for any purpose other than compliance with this Act or other provision of law, except where the recipient has given express consent.

(B) **OPT BACK IN.**— A prohibition in clause (i), (ii), or (iii) of subparagraph (A) does not apply if there is affirmative consent by the recipient subsequent to the request under subparagraph (A).

(5) **INCLUSION OF IDENTIFIER, OPT-OUT, AND PHYSICAL ADDRESS IN COMMERCIAL ELECTRONIC MAIL.**—

(A) It is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message provides—

(i) clear and conspicuous identification that the message is an advertisement or solicitation;

(ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender; and
(iii) a valid physical postal address of the sender.

(B) Subparagraph (A)(i) does not apply to the transmission of a commercial electronic mail if the recipient has given prior affirmative consent to receipt of the message.

(6) **SUBSEQUENT AFFIRMATIVE CONSENT.**— The prohibitions in subparagraphs (A), (B), and (C) do not apply to the initiation of transmission of commercial electronic mail to a recipient who, subsequent to a request using a mechanism provided pursuant to paragraph (3) not to receive commercial electronic mail messages from the sender, has granted affirmative consent to the sender to receive such messages.

(7) **MATERIALLY.**— For purposes of paragraph (1)(A), header information shall be considered to be materially misleading if it is altered or concealed in a manner that would impair the ability of an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to the person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message.

(b) **AGGRAVATED VIOLATIONS RELATING TO COMMERCIAL ELECTRONIC MAIL.**—

(1) **ADDRESS HARVESTING AND DICTIONARY ATTACKS.**—

(A) **IN GENERAL.**— It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message that is unlawful under subsection (a), or to assist in the origination of such message through the provision or selection of addresses to which the message will be transmitted, if such person had actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that—
(i) the electronic mail address of the recipient was obtained using an automated means from an Internet website or proprietary online service operated by another person, and such website or online service included, at the time the address was obtained, a notice stating that the operator of such website or online service will not give, sell, or otherwise transfer addresses maintained by such website or online service to any other party for the purposes of initiating, or enabling others to initiate, electronic mail messages; or
(ii) the electronic mail address of the recipient was obtained using an automated means that generates possible electronic mail addresses by combining names, letters, or numbers into numerous permutations.

(B) **DISCLAIMER.**—Nothing in this paragraph creates an ownership or proprietary interest in such electronic mail addresses.

(2) **AUTOMATED CREATION OF MULTIPLE ELECTRONIC MAIL ACCOUNTS.**—It is unlawful for any person to use scripts or other automated means to register for multiple electronic mail accounts or online user accounts from which to transmit to a protected computer, or enable another person to transmit to a protected computer, a commercial electronic mail message that is unlawful under subsection (a).

(3) **RELAY OR RETRANSMISSION THROUGH UNAUTHORIZED ACCESS.**—It is unlawful for any person knowingly to relay or retransmit a commercial electronic mail message that is unlawful under subsection (a) from a protected computer or computer network that such person has accessed without authorization.

(c) **SUPPLEMENTARY RULEMAKING AUTHORITY.**—The Commission shall by rule, pursuant to section 13—

(1) modify the 10-business-day period under subsection (a)(4)(A) or subsection (a)(4)(B), or both, if the Commission determines that a different period would be more reasonable after taking into account—

(A) the purposes of subsection (a);

(B) the interests of recipients of commercial electronic mail; and

(C) the burdens imposed on senders of lawful commercial electronic mail; and

(2) specify additional activities or practices to which subsection (b) applies if the Commission determines that those activities or practices are contributing substantially to the proliferation of commercial electronic mail messages that are unlawful under subsection (a).

(d) **REQUIREMENT TO PLACE WARNING LABELS ON COMMERCIAL ELECTRONIC MAIL CONTAINING SEXUALLY ORIENTED MATERIAL.**—

(1) **IN GENERAL.**—No person may initiate in or affecting interstate commerce the transmission, to a protected computer, of any commercial electronic mail message that includes sexually oriented material and—

(A) fail to include in subject heading for the electronic mail message the marks or notices prescribed by the Commission under this subsection; or

(B) fail to provide that the matter in the message that is initially viewable to the recipient, when the message is opened by any recipient and absent any further actions by the recipient, includes only—

(i) to the extent required or authorized pursuant to paragraph (2), any such marks or notices;

(ii) the information required to be included in the message pursuant to subsection (a)(5); and

(iii) instructions on how to access, or a mechanism to access, the sexually oriented material.

(2) **PRIOR AFFIRMATIVE CONSENT.**—Paragraph (1) does not apply to the transmission of an electronic mail message if the recipient has given prior affirmative consent to receipt of the message.

(3) **PRESCRIPTION OF MARKS AND NOTICES.**—Not later than 120 days after the date of the enactment of this Act, the Commission in consultation with the Attorney General shall prescribe clearly identifiable marks or notices to be included in or associated with commercial electronic mail that contains sexually oriented material, in order to inform the recipient of that fact and to facilitate filtering of such electronic mail. The Commission shall publish in the Federal Register and provide notice to the public of the marks or notices prescribed under this paragraph.

(4) **DEFINITION.**—In this subsection, the term “sexually oriented material” means

any material that depicts sexually explicit conduct (as that term is defined in section 2256 of title 18, United States Code), unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters.

(4) **PENALTY.**—Whoever knowingly violates paragraph (1) shall be fined under title 18, United States Code, or imprisoned not more than 5 years, or both.

SEC. 6. BUSINESSES KNOWINGLY PROMOTED BY ELECTRONIC MAIL WITH FALSE OR MISLEADING TRANSMISSION INFORMATION.

(a) **IN GENERAL.**—It is unlawful for a person to promote, or allow the promotion of, that person's trade or business, or goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business, in a commercial electronic mail message the transmission of which is in violation of section 5(a)(1) if that person—

(1) knows, or should have known in ordinary course of that person's trade or business, that the goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business were being promoted in such a message;

(2) received or expected to receive an economic benefit from such promotion; and

(3) took no reasonable action—

(A) to prevent the transmission; or

(B) to detect the transmission and report it to the Commission.

(b) **LIMITED ENFORCEMENT AGAINST THIRD PARTIES.**—

(1) **IN GENERAL.**—Except as provided in paragraph (2), a person (hereinafter referred to as the “third party”) that provides goods, products, property, or services to another person that violates subsection (a) shall not be held liable for such violation.

(2) **EXCEPTION.**—Liability for a violation of subsection (a) shall be imputed to a third party that provides goods, products, property, or services to another person that violates subsection (a) if that third party—

(A) owns, or has a greater than 50 percent ownership or economic interest in, the trade or business of the person that violated subsection (a); or

(B)(i) has actual knowledge that goods, products, property, or services are promoted in a commercial electronic mail message the transmission of which is in violation of section 5(a)(1); and

(ii) receives, or expects to receive, an economic benefit from such promotion.

(c) **EXCLUSIVE ENFORCEMENT BY FTC.**—Subsections (f) and (g) of section 7 do not apply to violations of this section.

(d) **SAVINGS PROVISION.**—Subject to section 7(f)(7), nothing in this section may be construed to limit or prevent any action that may be taken under this Act with respect to any violation of any other section of this Act.

SEC. 7. ENFORCEMENT GENERALLY.

(a) **VIOLATION IS UNFAIR OR DECEPTIVE ACT OR PRACTICE.**—Except as provided in subsection (b), this Act shall be enforced by the Commission as if the violation of this Act were an unfair or deceptive act or practice proscribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(b) **ENFORCEMENT BY CERTAIN OTHER AGENCIES.**—Compliance with this Act shall be enforced.

(1) under section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of—

(A) national banks, and Federal branches and Federal agencies of foreign banks, by the Office of the Comptroller of the Currency;

(B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 and 611), and bank holding companies, by the Board;

(C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System) insured State branches of foreign banks, by the Board of Directors of the Federal Deposit Insurance Corporation; and

(D) savings associations the deposits of which are insured by the Federal Deposit Insurance Corporation, by the Director of the Office of Thrift Supervision;

(2) under the Federal Credit Union Act (12 U.S.C. 1751 et seq.) by the Board of the National Credit Union Administration with respect to any Federally insured credit union;

(3) under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.) by the Securities and Exchange Commission with respect to any broker or dealer;

(4) under the Investment Company Act of 1940 (15 U.S.C. 80a-1 et seq.) by the Securities and Exchange Commission with respect to investment companies;

(5) under the Investment Advisers Act of 1940 (15 U.S.C. 80b-1 et seq.) by the Securities and Exchange Commission with respect to investment advisers registered under that Act;

(6) under State insurance law in the case of any person engaged in providing insurance, by the applicable State insurance authority of the State in which the person is domiciled, subject to section 104 of the Gramm-Bliley-Leach Act (15 U.S.C. 6701), except that in any State in which the State insurance authority elects not to exercise this power, the enforcement authority pursuant to this Act shall be exercised by the Commission in accordance with subsection (a);

(7) under part A of subtitle VII of title 49, United States Code, by the Secretary of Transportation with respect to any air carrier or foreign air carrier subject to that part;

(8) under the Packers and Stockyards Act, 1921 (7 U.S.C. 181 et seq.) (except as provided in section 406 of that Act (7 U.S.C. 226, 227)), by the Secretary of Agriculture with respect to any activities subject to that Act;

(9) under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.) by the Farm Credit Administration with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, or production credit association; and

(10) under the Communications Act of 1934 (47 U.S.C. 151 et seq.) by the Federal Communications Commission with respect to any person subject to the provisions of that Act.

(c) **EXERCISE OF CERTAIN POWERS.**—For the purpose of the exercise by any agency referred to in subsection (b) of its powers under any Act referred to in that subsection, a violation of this Act is deemed to be a violation of a Federal Trade Commission trade regulation rule. In addition to its powers under any provision of law specifically referred to in subsection (b), each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under this Act, any other authority conferred on it by law.

(d) **ACTIONS BY THE COMMISSION.**—The Commission shall prevent any person from violating this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade

Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any entity that violates any provision of that subtitle is subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act in the same manner, by the same means, and with the same jurisdiction, power, and duties as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of that subtitle.

(e) AVAILABILITY OF CEASE-AND-DESIST ORDERS AND INJUNCTIVE RELIEF WITHOUT SHOWING OF KNOWLEDGE.—Notwithstanding any other provision of this Act, in any proceeding or action pursuant to subsection (b), (c), or (d) of this section to enforce compliance, through an order to cease and desist or an injunction, with section 5(a)(2), subparagraph (B) or (C) of section 5(a)(4), or section 5(b)(1)(A), neither the Commission nor the Federal Communications Commission shall be required to allege or prove the state of mind required by such section or subparagraph.

(f) ENFORCEMENT BY STATES.—

(1) CIVIL ACTION.—In any case in which the attorney general of a State, or an official or agency of a State, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any person who violates paragraph (1) or (2) of section 5(a), or who engages in a pattern or practice that violates paragraph (3), (4), or (5) of section 5(a) of this Act, the attorney general, official, or agency of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction.

(A) to enjoin further violation of section 5 of this Act by the defendant; or

(B) to obtain damages on behalf of residents of the State, in an amount equal to the greater of—

(i) the actual monetary loss suffered by such residents; or

(ii) the amount determined under paragraph (2).

(2) AVAILABILITY OF INJUNCTIVE RELIEF WITHOUT SHOWING OF KNOWLEDGE.—Notwithstanding any other provision of this Act, in a civil action under paragraph (1)(A) of this subsection, the attorney general, official, or agency of the State shall not be required to allege or prove the state of mind required by section 5(a)(2), subparagraph (B) or (C) of section 5(a)(4), or section 5(b)(1)(A).

(3) STATUTORY DAMAGES.—

(A) IN GENERAL.—For purposes of paragraph (1)(B)(ii), the amount determined under this paragraph is the amount calculated by multiplying the number of violations (with each separately addressed unlawful message received by or addressed to such residents treated as a separate violation) by up to \$250.

(B) LIMITATION.—For any violation of section 5 (other than section 5(a)(1)), the amount determined under subparagraph (A) may not exceed \$2,000,000.

(C) AGGRAVATED DAMAGES.—The court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this paragraph if—

(i) the court determines that the defendant committed the violation willfully and knowingly; or

(ii) the defendant's unlawful activity included one or more of the aggravating violations set forth in section 5(b).

(D) REDUCTION OF DAMAGES.—In assessing damages under subparagraph (A), the court may consider whether—

(i) the defendant has established and implemented, with due care, commercially rea-

sonable practices and procedures to effectively prevent such violations; or

(ii) the violation occurred despite commercially reasonable efforts to maintain compliance with such practices and procedures.

(3) ATTORNEY FEES.—In the case of any successful action under paragraph (1), the State may be awarded the costs of the action and reasonable attorney fees as determined by the court.

(4) RIGHTS OF FEDERAL REGULATORS.—The State shall serve prior written notice of any action under paragraph (1) upon the Federal Trade Commission or the appropriate Federal regulator determined under subsection (b) and provide the Commission or appropriate Federal regulator with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case the State shall serve such notice immediately upon instituting such action. The Federal Trade Commission or appropriate Federal regulator shall have the right—

(A) to intervene in the action;

(B) upon so intervening, to be heard on all matters arising therein;

(C) to remove the action to the appropriate United States district court; and

(D) to file petitions for appeal.

(5) CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this Act shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under paragraph (1) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under paragraph (1), process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) maintains a physical place of business.

(7) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission or other appropriate Federal agency under subsection (b) has instituted a civil action or an administrative action for violation of this Act, no State attorney general, or official or agency of a State, may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the Commission or the other agency for any violation of this Act alleged in the complaint.

(8) REQUISITE SCIENTER FOR CERTAIN CIVIL ACTIONS.—Except as provided in subsections (a)(2), (a)(4)(B), (a)(4)(C), (b)(1), and (d) of section 5, and paragraph (2) of this subsection, in a civil action brought by a State attorney general, or an official or agency of a State, to recover monetary damages for a violation of this Act, the court shall not grant the relief sought unless the attorney general, official, or agency establishes that the defendant acted with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, of the act or omission that constitutes the violation.

(9) ACTION BY PROVIDER OF INTERNET ACCESS SERVICE.—

(1) ACTION AUTHORIZED.—A provider of Internet access service adversely affected by a violation of section 5(a) or of section 5(b), or a pattern or practice that violated paragraph (2), (3), (4), or (5) of section 5(a), may bring a civil action in any district court of the United States with jurisdiction over the defendant—

(A) to enjoin further violation by the defendant; or

(B) to recover damages in an amount equal to the greater of—

(i) actual monetary loss incurred by the provider of Internet access service as a result of such violation; or

(ii) the amount determined under paragraph (3).

(2) SPECIAL DEFINITION OF "PROCURE".—In any action brought under paragraph (1), this Act shall be applied as if the definition of the term "procure" in section 3(12) contained, after "behalf" the words "with actual knowledge, or by consciously avoiding knowing, whether such person is engaging, or will engage, in a pattern or practice that violates this Act".

(3) STATUTORY DAMAGES.—

(A) IN GENERAL.—For purposes of paragraph (1)(B)(ii), the amount determined under this paragraph is the amount calculated by multiplying the number of violations (with each separately addressed unlawful message that is transmitted or attempted to be transmitted over the facilities of the provider of Internet access service, or that is transmitted or attempted to be transmitted to an electronic mail address obtained from the provider of Internet access service in violation of section 5(b)(1)(A)(i), treated as a separate violation) by—

(i) up to \$100, in the case of a violation of section 5(a)(1); or

(ii) \$25, in the case of any other violation of section 5.

(B) LIMITATION.—For any violation of section 5 (other than section 5(a)(1)), the amount determined under subparagraph (A) may not exceed \$1,000,000.

(C) AGGRAVATED DAMAGES.—The court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this paragraph if—

(i) the court determines that the defendant committed the violation willfully and knowingly; or

(ii) the defendant's unlawful activity included one or more of the aggravated violations set forth in section 5(b).

(D) REDUCTION OF DAMAGES.—In assessing damages under subparagraph (A), the court may consider whether—

(i) the defendant has established and implemented, with due care, commercially reasonable practices and procedures to effectively prevent such violations; or

(ii) the violation occurred despite commercially reasonable efforts to maintain compliance with such practices and procedures.

(4) ATTORNEY FEES.—In any action brought pursuant to paragraph (1), the court may, in its discretion, require an undertaking for the payment of the costs of such action, and assess reasonable costs, including reasonable attorneys' fees, against any party.

SEC. 8. EFFECT ON OTHER LAWS.

(a) FEDERAL LAW.—

(1) Nothing in this Act shall be construed to impair the enforcement of section 233 or 231 of the Communications Act of 1934 (47 U.S.C. 223 or 231, respectively), chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code, or any other Federal criminal statute.

(2) Nothing in this Act shall be construed to affect in any way the Commission's authority to bring enforcement actions under FTC Act for materially false or deceptive representations or unfair practices in commercial electronic mail messages.

(b) STATE LAW.—

(1) IN GENERAL.—This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send

commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.

(2) STATE LAW NOT SPECIFIC TO ELECTRONIC MAIL.- This Act shall not be construed to preempt the applicability of-

(A) State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or

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

(c) NO EFFECT ON POLICIES OF PROVIDERS OF INTERNET ACCESS SERVICE.- Nothing in this Act shall be construed to have any effect on the lawfulness or unlawfulness, under any other provision of law, of the adoption, implementation, or enforcement by a provider of Internet access service of a policy of declining to transmit, route, relay, handle, or store certain types of electronic mail messages.

SEC. 9. DO-NOT-E-MAIL REGISTRY.

(a) IN GENERAL.- Not later than 6 months after the date of enactment of this Act, the Commission shall transmit to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce a report that-

(1) sets forth a plan and timetable for establishing a nationwide marketing Do-Not-E-mail registry;

(2) includes an explanation of any practical, technical, security, privacy, enforceability, or other concerns that the Commission has regarding such a registry; and

(3) includes an explanation of how the registry would be applied with respect to children with e-mail accounts.

(b) AUTHORIZATION TO IMPLEMENT.- The Commission may establish and implement the plan, but not earlier than 9 months after the date of enactment of this Act.

SEC. 10. STUDY OF EFFECTS OF COMMERCIAL ELECTRONIC MAIL.

(a) IN GENERAL.- Not later than 24 months after the date of the enactment of this Act, the Commission, in consultation with the Department of Justice and other appropriate agencies, shall submit a report to the Congress that provides a detailed analysis of the effectiveness and enforcement of the provisions of this Act and the need (if any) for the Congress to modify such provisions.

(b) REQUIRED ANALYSIS.- The Commission shall include in the report required by subsection (a)-

(1) an analysis of the extent to which technological and marketplace developments, including changes in the nature of the devices through which consumers access their electronic mail messages, may affect the practicality and effectiveness of the provisions of this Act;

(2) analysis and recommendations concerning how to address commercial electronic mail that originates in or is transmitted through or to facilities or computers in other nations, including initiatives or policy positions that the Federal government could pursue through international negotiations, fora, organizations, or institutions; and

(3) analysis and recommendations concerning options for protecting consumers, including children, from the receipt and viewing of commercial electronic mail that is obscene or pornographic.

SEC. 11. IMPROVING ENFORCEMENT BY PROVIDING REWARDS FOR INFORMATION ABOUT VIOLATIONS; LABELING.

The Commission shall transmit to the Senate Committee on Commerce, Science, and

Transportation and the House of Representatives Committee on Energy and Commerce-

(1) a report, within 9 months after the date of enactment of this Act, that sets forth a system for rewarding those who supply information about violations of this Act, including-

(A) procedures for the Commission to grant a reward of not less than 20 percent of the total civil penalty collected for a violation of this Act to the first person that-

(i) identifies the person in violation of this Act; and

(ii) supplies information that leads to the successful collection of a civil penalty by the Commission; and

(B) procedures to minimize the burden of submitting a complaint to the Commission concerning violations of this Act, including procedures to allow the electronic submission of complaints to the Commission; and

(2) a report, within 18 months after the date of enactment of this Act, that sets forth a plan for requiring commercial electronic mail to be identifiable from its subject line, by means of compliance with Internet Engineering Task Force Standards, the use of the characters "ADV" in the subject line, or other comparable identifier, or an explanation of any concerns the Commission has that cause the Commission to recommend against the plan.

SEC. 12. RESTRICTIONS ON OTHER TRANSMISSIONS.

Section 227(b)(1) of the Communications Act of 1934 (47 U.S.C. 227(b)(1)) is amended, in the matter preceding subparagraph (A), by inserting ", or any person outside the United States if the recipient is within the United States" after "United States".

SEC. 13. REGULATIONS.

(a) IN GENERAL.- The Commission may issue regulations to implement the provisions of this Act (not including the amendments made by sections 4 and 12). Any such regulations shall be issued in accordance with section 553 of title 5, United States Code.

(b) LIMITATION.- Subsection (a) may not be construed to authorize the Commission to establish a requirement pursuant to section 5(a)(5)(A) to include any specific words, characters, marks, or labels in a commercial electronic mail message, or to include the identification required by section 5(a)(5)(A) in any particular part of such a mail message (such as the subject line or body).

SEC. 14. APPLICATION TO WIRELESS.

(a) EFFECT ON OTHER LAW.- Nothing in this Act shall be interpreted to preclude or override the applicability of section 227 of the Communications Act of 1934 (47 U.S.C. 227) or the rules prescribed under section 3 of the Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. 6102). To the extent that a requirement of such Acts, or rules or regulations promulgated thereunder, is inconsistent with the requirement of this Act, the requirement of such other Acts, or rules or regulations promulgated thereunder, shall take precedence.

(b) FCC RULEMAKING.- The Federal Communications Commission, in consultation with the Federal Trade Commission, shall promulgate rules within 270 days to protect consumers from unwanted mobile service commercial messages. The rules shall, to the extent consistent with subsection (c)-

(1) provide subscribers to commercial mobile services the ability to avoid receiving mobile service commercial messages unless the subscriber has provided express prior authorization, except as provided in paragraph (3);

(2) allow recipients of mobile service commercial messages to indicate electronically a desire not to receive future mobile service commercial messages from the initiator;

(3) take into consideration, in determining whether to subject providers of commercial mobile wireless services to paragraph (1), the relationship that exists between providers of such services and their subscribers, but if the Commission determines that such providers should not be subject to paragraph (1), the rules shall require such providers, in addition to complying with the other provisions of this Act, to allow subscribers to indicate a desire not to receive future mobile service commercial messages at the time of subscribing to such service, and in any billing mechanism; and

(4) determine how initiators of mobile service commercial messages may comply with the provisions of this Act, considering the unique technical aspects, including the functional and character limitations, of devices that receive such messages.

(c) OTHER FACTORS CONSIDERED.- The Federal Communications Commission shall consider the ability of an initiator of an electronic mail message to reasonably determine that the electronic mail message is a mobile service commercial message.

(d) MOBILE SERVICE COMMERCIAL MESSAGE DEFINED.- In this section, the term "mobile service commercial message" means a commercial electronic mail message that contains text, graphics, or images for visual display that is transmitted directly to a wireless device that-

(1) is utilized by a subscriber of commercial mobile service (as such term is defined in section 332(d) of the Communications Act of 1934 (47 U.S.C. 332(d)) in connection with such service; and

(2) is capable of accessing and displaying such a message.

SEC. 15. SEPARABILITY.

If any provision of this Act or the application thereof to any person or circumstance is held invalid, the remainder of this Act and the application of such provision to other persons or circumstances shall not be affected.

SEC. 16. EFFECTIVE DATE.

The provisions of this Act, other than section 9, shall take effect on January 1, 2004.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Louisiana (Mr. TAUZIN) and the gentleman from Massachusetts (Mr. MARKEY) each will control 20 minutes.

The Chair recognizes the gentleman from Louisiana (Mr. TAUZIN).

GENERAL LEAVE

Mr. TAUZIN, Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and to insert extraneous material on S. 877.

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

There was no objection.

Mr. TAUZIN, Mr. Speaker, I ask unanimous consent that the gentleman from Wisconsin (Mr. SENSENBRENNER) be given control of 10 minutes of my time.

The SPEAKER pro tempore. Without objection, the request of the gentleman from Louisiana is granted.

There was no objection.

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

Mr. Speaker, for the second time in just a few months, Congress is on the verge of passing watershed consumer protection legislation. Less than 2

months ago, we enacted, in record time I might add, legislation that codified the ability of the Federal Trade Commission to implement the Do Not Call Registry on telemarketing phone calls. Today, we take an equivalent step in the Internet area. S. 877, with the substitute I have called up, will give millions of Americans the ability to block unwanted and unsolicited commercial e-mail, what we now derisively call spam.

The Internet has given us abilities beyond our wildest dreams; and as it continues to grow in popularity and functionality, the time will come when every American, from school kids to senior citizens, homemakers to CEOs, will rely on it for crucial aspects of their lives. I received, by the way, my first e-mail from my mom just this month. And she was thrilled, and I was thrilled to see her enter the Internet Age.

But one of the terrific aspects of the Internet, the ability to send and receive e-mail, has given us enormous headaches because of spam. It cripples computer networks and makes regular e-mail checking a seemingly endless hassle.

□ 1715

Even worse, a great deal of spam channels in pornography and other subjects not worthy of discussion on a family cable channel, and this spam frequently preys on defenseless, unsuspecting children.

Well, we are here to provide the necessary tools to end the nonsense and to bring some peace of mind back to parents around the country. The substitute before us will empower American consumers with a right to opt out of all unwanted, unsolicited commercial e-mail, or spam, and it will also provide the Federal Trade Commission with the authority to set up a Do-Not-Spam Registry based upon the Do-Not-Call Registry. The substitute grants strong protection for parents and consumers to say no to the receipt of pornographic spam, and makes it a crime subject to 5 years in prison to send fraudulent spam. And finally, it gives the FTC and State attorneys general the ability to vigorously enforce the new law.

I am pleased to report that the product before us now enjoys broad bipartisan support here in the House and also in the other body. The bill can and should go to President Bush before we adjourn the first session of the 108th Congress. Mr. Speaker, I urge my colleagues to vote for this much-needed, bipartisan bill.

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

Mr. MARKEY. Mr. Speaker, I yield 2 minutes to the gentleman from Texas (Mr. GREEN).

Mr. GREEN of Texas. Mr. Speaker, I would like to thank our ranking member on the Subcommittee on Telecommunications and the Internet for yielding me this time.

I rise in strong support of S. 877, the compromise which has been worked out on the antispam legislation.

First, I want to thank the gentlewoman from New Mexico (Mrs. WILSON) for the many years of work she has put in with me and other members of the Committee on Energy and Commerce.

I also thank the leadership of our committee, the ranking member, the gentleman from Michigan (Mr. DINGELL) and the gentleman from Louisiana (Chairman TAUZIN) for their strong commitment to this effort which the gentlewoman from New Mexico (Mrs. WILSON) and I began almost 5 years ago. She had a terrible personal experience with spam, and I heard from constituents some of the same stories, and my wife and I have received some of that same unsolicited spam on our own personal e-mail account.

This legislation will set the fair and clear standards for e-mail marketing that consumers and the Internet need desperately. The future of e-mail is at stake, and the time to act is now. Congress is delivering the enforcement tools we need.

Importantly, this compromise has clear definitions of commercial e-mail which the FTC can enforce and any individual consumer's request to not receive further commercial e-mail from a sender will have the force of the law. Spammers who lie and deceive with false header information and deceptive subject lines will be lawbreakers and will be prosecuted as such.

After we enact this legislation, spammers will no longer be able to harvest e-mail addresses from Web pages across the Internet without the threat of prosecution. There are so many good things in this bill that it is hard to go over all of them in 2 minutes.

We will come after spammers from all angles. State attorneys general are empowered, and Internet service providers are empowered to seek damages up to \$250 per e-mail or \$6 million total.

After the success of the FTC's Do-Not-Call list, the Do-Not-Spam registry implementation is feasible. I thank the gentleman from Louisiana (Mr. TAUZIN) and our ranking member, and I also thank the many cosponsors of our original bill, H.R. 2515, on the antispam effort.

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

Mr. Speaker, I rise in support of the House-modified version of Senate 877, and wish to thank my fellow chairman, the gentleman from Louisiana (Mr. TAUZIN), as well as the gentleman from Michigan (Mr. DINGELL) and the gentleman from Massachusetts (Mr. MARKEY) in working out this compromise which deals with a very vexatious question, and I think provides a win/win situation for everybody except the few bad actors that flood the electronic media with spam.

The Internet has revolutionized commerce and communications by permit-

ting businesses to reach consumers in a digital, global marketplace and has allowed individuals to communicate through the speed and convenience of electronic mail. Unfortunately, the massive growth of unsolicited e-mail or "spam" now threatens to kill the utility of this popular media. Last year over 6 trillion e-mails were transmitted. Today, almost half of those e-mails are unsolicited or unwanted.

Commercial e-mail is good, and a necessary and valuable component of electronic commerce. It allows legitimate businesses to customize offers of products and services and transmit them immediately to customers.

However, the same features that make e-mail a valuable commercial tool also lead to its abuse by spammers. Once a portable to the global network is obtained, sending e-mail is instantaneous and virtually costless. There are no stamps in cyberspace, no per-message cost, not even a post office. The costs of delivery are borne more by the recipient and the transmission network than by the sender. The exponential growth of spam and the advancing sophistication of efforts to block it threaten to turn the information superhighway into a nightmare for every info-commuter and parent.

Like other means of communication, e-mail can be used to cheat, defraud, and deceive consumers and also has been used to distribute computer viruses that have caused millions of dollars in economic damages. Unscrupulous spammers have transformed electronic inboxes and the Internet into virtual minefields strewn with lewd and pornographic images and solicitations, imperiling a medium that can serve as a critical learning tool for children.

I am pleased to support this version of Senate 877, which is substantially similar to H.R. 2214 introduced by the gentleman from North Carolina (Mr. BURR), the gentleman from Louisiana (Mr. TAUZIN) and myself earlier this year. I believe it will provide a remedial enforcement mechanism that private, regulatory, and individual State action cannot.

The criminal provisions contained in this legislation are central to its purpose and to its effectiveness. In order to provide a credible deterrent to spammers, this legislation enhances criminal penalties for predatory spamming, and provides law enforcement personnel far more authority to prosecute spammers whose electronic presence can shift with a keystroke.

The bill provides significant criminal penalties for the most egregious spammers by making it a crime to intentionally falsify the identity of the sender or disguise the routing and source information of e-mails. Other spammer tactics made criminal under this bill include the hijacking protected computers to send spam from the addresses of unsuspecting Internet users.

The House modification of S. 877 also provides for much higher penalties and

more effective civil and criminal enforcement against spammers who send unwanted sexually explicit materials. This bill even requires special labels for this most offensive category of e-mail. The gentlewoman from Pennsylvania (Ms. HART) deserves special recognition for her work to get this provision into law.

Overall, the bill provides consumers with more information and choices to stop receiving all forms of unwanted commercial e-mail while providing law enforcement officials and providers of Internet access with the tools to go after spammers.

While S. 877 accomplishes these vital goals, there are some activities that it deliberately does not reach. Specifically, the legislation concerns only commercial and sexually explicit e-mail and is not intended to intrude on the burgeoning use of e-mail to communicate for political, news, personal and charitable purposes.

Moreover, this legislation, while preempting State spam specific laws with a uniform national standard, also preserves a role for State law enforcement officials to help combat this growing electronic menace. The bill also allows for State laws that deal with fraud and computer crimes to remain in effect. However, there is specific language in the bill limiting this authority to law enforcement officials or agencies of the State, and it is not the intent of Congress to allow outsourcing of this truly State function to the plaintiff's bar.

The House-modified legislation also contains other necessary amendments to the bill passed by the other body and reflects a thoughtful, bipartisan and bicameral approach to address the growing scourge of spam while preserving and promoting the commercial vitality of the Internet. I urge my colleagues to support this legislation.

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

Mr. MARKEY. Mr. Speaker, I yield myself 2½ minutes.

Mr. Speaker, this is a very important bill, and it would not have been possible without the good work of the gentleman from Louisiana (Mr. TAUZIN) and his staff, David Cavicke, along with the gentleman from Michigan (Mr. DINGELL) and his staff, David Schooner and Gregg Rothschild, working with the majority. I think we have come to an excellent result. It builds upon the work that the gentlewoman from New Mexico (Mrs. WILSON) and the gentleman from Texas (Mr. GREEN) have been making for years in this area. I think that the public is really going to be a beneficiary from this product this evening. I would be remiss, of course, not to single out the gentleman from Wisconsin (Mr. SENSENBRENNER) as well and his staff for their excellent work on this bill.

In addition to the other provisions mentioned by other Members, this legislation now contains a modified version of the wireless spam amendment that I had offered for inclusion.

The legislation preserves important authority of the Federal Communications Commission and FTC where it serves consumer interests. It also requires the FCC to initiate a rule-making for wireless spam so that no loopholes are created, but in a way to ensure that wireless consumers have greater protection than that accorded in the underlying bill.

As we attempt to tackle the issue of spam that is sent to our desktop computers, we must also recognize that millions of wireless consumers in the United States run the risk of being inundated by wireless spam. Unsolicited wireless text messages have plagued wireless users in Europe, South Korea and Japan over the last few years as wireless companies in such countries have offered wireless messaging services.

In Japan alone, NTT DoCoMo estimates that its wireless network processes some 800 million wireless spam messages a day. That is a day. As cumbersome and annoying as spam to a desktop computer is, at least a consumer can turn off their computer and walk away. Wireless spam is even more intrusive because spam to wireless phones is the kind of spam that follows you wherever you go, and according to the U.S. wireless carriers, is already on the rise.

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

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

Mr. Speaker, I thank the gentleman from Massachusetts for thanking the majority staff. I wish I could introduce Mr. Cavicke because he has done such a great job on this bill, but he is not a Member.

Mr. Speaker, I yield 2 minutes to the gentlewoman from New Mexico (Mrs. WILSON) to speak on the bill.

Mrs. WILSON of New Mexico. Mr. Speaker, 5 years ago spam was a nuisance, and now it is a nightmare. It is interrupting people's legitimate use of the Internet and their ability to communicate without having a lot of junk to go through every morning.

I think today is a great victory for consumers and for parents. Parents should not have to worry about the kinds of things coming into their kids' inboxes. For the first time, Americans who use the Internet and get e-mail will have the right to say take me off your list. I do not want this in my house. That is a tremendous right to be given to citizens in this Nation.

I am glad we have a strong bill with strong enforcement that requires labels for sexually explicit material, and allows users to opt out without having things that are required to be viewed in order to do so.

E-mail has been called the "killer app" of the Internet, the killer application. And now today, we are saying that the people who use it are going to have the right to take it back and own it without an encumbrance by spammers.

Mr. Speaker, I want to thank the gentleman from Louisiana (Mr. TAUZIN), the gentleman from Wisconsin (Mr. SENSENBRENNER), the gentleman from Texas (Mr. GREEN) with whom I have been working on this issue for over 4 years, and the gentleman from Michigan (Mr. DINGELL) who has also been a wonderful leader in this effort, as well as the gentlewoman from Pennsylvania (Ms. HART) and the gentleman from North Carolina (Mr. BURR) for their efforts. We have put together a good bill, and it is a better bill because we have all worked on it together.

Mr. MARKEY. Mr. Speaker, I yield 2 minutes to the gentleman from Texas (Mr. GREEN).

Mr. GREEN of Texas. Mr. Speaker, I would like to talk about some of the good things about this agreement that is in the bill S. 877.

Spammers who lie and deceive with false header information and deceptive subject lines will be lawbreakers and prosecuted. After we enact this legislation, spammers will no longer be able to harvest e-mail addresses from Web pages across the Internet without the threat of prosecution.

□ 1730

Our bill cracks down on automated "dictionary" spam attacks, the spam version of the auto-dialer that sends spam to every possible e-mail combination. Most importantly for our families, and something that the gentlewoman from New Mexico (Mrs. WILSON) experienced with her daughter, this bill requires warning labels on sexually explicit e-mail; and we will be able to refuse further e-mail without having to view the offensive content. It will go after spammers again from all angles, from the Federal Trade Commission, from the States attorneys general and also Internet service providers who, as the gentleman from Wisconsin (Mr. SENSENBRENNER) said, 50 percent of the networks oftentimes are unsolicited e-mail. They will be able to sue for damages of \$250 per e-mail or a total of \$6 million. It is there so our attorneys general have the ability and our ISPs will do it.

Finally, after the success of the Do-Not-Call list, the FTC is to plan a Do-Not-Spam registry within 6 months and will implement it if it is feasible.

Like my colleagues, our staff worked hard on it in both our committees, Judiciary and Energy and Commerce. I thank my personal staff, Drew Wallace, for working on this with all the folks involved.

Mr. SENSENBRENNER. Mr. Speaker, I yield 2 minutes to the gentleman from Virginia (Mr. GOODLATTE).

Mr. GOODLATTE. Mr. Speaker, I thank the gentleman from Wisconsin, chairman of the Committee on the Judiciary, and the gentleman from Louisiana, chairman of the Committee on Energy and Commerce, for their leadership in pulling these two committees together. We have been working on this

for a long time. It is that kind of teamwork that has resulted in this legislation today as well as a great deal of cooperation on the other side of the aisle. We really appreciate what it takes to write good legislation.

Spam is not just a nuisance anymore. Over half of the e-mail sent today is spam. Unsolicited e-mail, such as advertisements, solicitations, or chain letters is the junk mail of the Information Age. At best these unwanted messages burden consumers by slowing down their e-mail connections. At worst these messages bombard American families with unsolicited, sexually explicit materials and fraudulent information. It is time to can spam.

The bill before us makes it a criminal offense to send a commercial e-mail that falsifies the sender's identity. In addition, the House amendments which have been incorporated into this bill strengthen the provisions that punish spammers for failing to place warning labels on sexually explicit materials.

This bill makes the necessary changes to the Senate's "can spam act" to establish clear, uniform guidelines for those who send commercial e-mail and to criminalize fraudulent conduct. The bill provides State attorneys general, ISPs, the FTC, and the Department of Justice with the appropriate tools to enforce the bill against bad actors.

Because no legislation can provide a cure-all for spam, this bill is technology-friendly. It protects the ability of ISPs and small businesses to develop innovative technological solutions to combat spam and to protect consumers, such as filtering and blocking technologies. This bill establishes clear guidelines for legitimate businesses and punishes fraudulent conduct, not going after the good guys. It accomplishes these objectives without over-regulating and without taking the information out of the Information Age.

I urge my colleagues to support this important legislation.

Mr. MARKEY. Mr. Speaker, I yield 5 minutes to the gentleman from Michigan (Mr. DINGELL), the ranking Democrat on the Committee on Energy and Commerce.

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

Mr. DINGELL. Mr. Speaker, we can work well together around here. I am sure that a lot of people are surprised.

I want to pay a congratulations and compliment to my distinguished friend, the gentleman from Louisiana (Mr. TAUZIN), the chairman of the committee, and also to the distinguished gentleman from Wisconsin (Mr. SENBRENNER) for his labors. I want to thank my good friend, the gentleman from Massachusetts (Mr. MARKEY), for his leadership in this valiant effort and undertaking, and I want to pay particular tribute to both the distinguished gentleman from Texas (Mr. GREEN) and the wonderful gentle-

woman from New Mexico (Mrs. WILSON) for their outstanding leadership, for the courage and for the dedication with which they stood hitched on this difficult issue and these difficult negotiations. Congratulations to all of the above. And also to Mr. Gregg Rothschild, Mr. David Cavicke, Mr. Bryce Dustman, and Peter Filon of the staff; also David Schooler and Shannon Vildostegui for their wonderful work as members of the staff because their efforts have helped make this possible.

This is a good bill and it is worthy of our support. There are things that we could have done that would have been a little better, but it is a piece of legislation which is going to solve a concern of the American people, something which is good and is in the public interest. And it is an important first step in restoring consumers' control over their inboxes and stopping some of the evil and rascality that we are seeing in the telecommunications industry. It requires marketers to let people know who they are and where they can be located. It prohibits false and misleading transmission information so that marketers cannot hide their identity. It prohibits marketers from deceiving consumers by using false headers or subject lines. Importantly, it affords the Federal Trade Commission and the States full enforcement authority over these consumer protection provisions.

I am particularly pleased that the bill permits law enforcement to go after those who disguise sexual messages and through such deception are able to send sexual material into our homes and into the hands of our children. This is a critical first step against those who profit by sending unwanted and offensive sexual commercial messages. It will stop much wrongdoing.

I am also pleased that the House has adopted the Senate provision creating a do-not-spam registry. I expect the FTC to take their charge seriously under this provision and to do all that is necessary to implement such a registry at the earliest possible time.

Finally, I am pleased that the House has added a new provision to grant even stronger protections from spam to users of wireless cell phones. The gentleman from Massachusetts deserves the thanks of all of us for that. In connection with this provision, I commend the hard work of our dear friend, the ranking Democrat on the Subcommittee on Telecommunications and the Internet.

Mr. Speaker, I want to be clear that I do not expect this bill to solve totally the growing problem of unwanted spam. It must be recognized that the people who engage in this practice are most diligent, most able, and have a huge financial incentive to do it. It is quite possible that we will have to visit the matter again. It is regrettable that it does not contain an important deterrence against spam, citizen suits; but we can address that at a future time. It also has the regrettable practice in it

of preempting stronger State laws, something which I do not favor. It is, however, a distinct improvement over the Senate-passed bill, and the hard work that has brought us to agreement on the part of those who have worked on it is something which merits the thanks of the public for work in the public interest.

I plan to work to try and expand this in future times and to do the things that are necessary to assure that our people are not abused by these people.

Mr. TAUZIN. Mr. Speaker, I thank the distinguished gentleman from Michigan for his statement and his kind friendship.

Mr. Speaker, I yield 2 minutes to the distinguished gentleman from Michigan (Mr. UPTON), chairman of the Subcommittee on Telecommunications and the Internet.

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

Mr. UPTON. Mr. Speaker, today on the heels of our recent efforts to ensure that the do-not-call list was implemented, we are taking yet another major step forward in our efforts to protect consumers from unwanted commercial solicitations. With passage of this bill tonight, we are one more step closer to giving American consumers a Federal law which will for the first time allow them to just say no to unwanted commercial e-mails, otherwise known as spam. And we back it up with strong enforcement by the FTC, State attorneys general, and Internet service providers as well.

As the father of two young kids, I am particularly pleased that this bill requires warning labels on commercial e-mails which contain sexually oriented material, and it protects our kids from being unwittingly exposed to such garbage that might pop up in the family's inbox. As chairman of the Subcommittee on Telecommunications and the Internet, I am particularly pleased to have worked with my colleagues on this, particularly the gentleman from Massachusetts (Mr. MARKEY); the gentleman from Michigan (Mr. DINGELL); certainly the gentleman from North Carolina (Mr. BURR); and my chairman, the gentleman from Louisiana (Mr. TAUZIN), on provisions which direct the Federal Communications Commission to implement added protections against spam for cell phones and other wireless devices. What a nightmare ready to happen. On our staff I want to particularly thank Will Nordwind, who spent countless hours as we negotiated this the last number of months.

Mr. Speaker, I want to relate a small family story. When my dad came back from World War II, my mom fixed his first dinner. It was Spam. Dad said, no way. Battle of the Bulge, we had enough of that. No more are we going to have that junk. My family thankfully was spared that for 50 years. Sadly, American consumers have not been spared from that awful stuff called spam because this is spam on the Internet.

I can remember when e-mails came first off, everyone loved to get an e-mail. I thought we were finally making some headway. But lo and behold, my wife was out of town, and I did not realize she was deleting it. Every morning she would get up at 5:30 or 6 in the morning. She has been gone all week. Today just from last night, I had 150 spams.

Pass this bill. End this stuff. I cannot call it what I really think. God bless America.

Mr. MARKEY. Mr. Speaker, I yield 1 additional minute to the gentleman from Texas (Mr. GREEN).

Mr. GREEN of Texas. Mr. Speaker, I know we are getting down to the last few minutes, but, like my colleague from Michigan, I ate a lot of Spam. I am holding up my gift of Spam from my cosponsor. Like him, the only way I could ever survive Spam was with A-1 steak sauce. I remember the story that my first time, somebody showing up at a town hall meeting and saying, I'm tired of spam and I said, thank goodness I haven't had to eat it in years. But I do remember it tasted pretty good in college when I needed it.

But now as my colleague from Michigan said, spam will not have a bad name for people who use the Internet. Again, I would like to thank the gentleman from New Mexico (Mrs. WILSON) for providing me a can of Spam. I am not going to cook it. I am going to put it on the wall so hopefully I will not have to.

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

Mr. Speaker, after hearing about that stuff that the gentleman from Texas was waving around, let me say that we Yankees knew that Spam was bad 50 years ago. It has taken a long time for you rebels to do that.

Mr. Speaker, I yield 1 minute to the gentleman from Pennsylvania (Ms. HART).

Ms. HART. Mr. Speaker, I also thank the gentleman from Wisconsin (Mr. SENSENBRENNER), the gentleman from Louisiana (Mr. TAUZIN), the gentleman from Michigan (Mr. DINGELL), and the general public, really, for helping us move this bill forward. I am pleased we were able to work out a deal on this legislation. It has taken some time, but the product is well worth it. The American public has been flooded with millions of pieces of unsolicited e-mail every day. This legislation will help us provide the teeth in the law to stop this. But it is the content of certain e-mails, particularly e-mails containing sexually explicit material which is especially problematic.

I compliment the gentleman from New Mexico (Mrs. WILSON) for working together with us on language that is similar to the Pennsylvania law that I sponsored to help label and help us rid our computers of these sexually explicit e-mails. I am pleased this was put into the bill. We want our children to use the Internet and e-mail, but

many parents fear what the children may see. Parents are stuck in the middle. They want their kids to use the educational tool of the Internet, they want them to be very capable of utilizing it, and it will help them in their schoolwork on one hand, but on the other when my Senator was sitting behind one of his children, in fact, he said to me, I could not believe what came up on the screen.

It is important for us to make sure that we control it but we allow freedom of speech. I compliment my colleagues. I look forward to a spam-free e-mail.

Mr. MARKEY. Mr. Speaker, I yield myself 2 minutes.

The reality is that this whole movement began as people several years ago saw what the impact would be of unwanted spam on their home or work computers. As the gentleman from Michigan (Mr. UPTON) pointed out, he had in one day 150 unwanted spam messages on his home computer. What this legislation does is to help every American to deal with that problem. What I ask the Members to do as well is to deal with another issue that quite likely is going to rise to a level of being a problem that eclipses even computer spam and that would be cell phone spam.

Imagine if you reach a point where there are 150 unwanted rings on your phone, your cell phone, this zone of privacy which we all have as these marketers are calling into your cell phone all day long. What this legislation does is it ensures that the Federal Communications Commission and the Federal Trade Commission take the actions which give protections against this being the new battleground. It is already a full scale epidemic in Europe, in Japan, in South Korea.

□ 1745

It is heading our way. Probably by the time the FCC has a chance to put the regulations on the books, maybe a year from now, we will have already seen its growth so those protections against these cell phones just ringing all day long becomes the epidemic that really just drives people crazy. So the bill will require the FCC to consider certain provisions with an eye towards assessing the problems and perhaps the unique capabilities or limitations of wireless devices. We have to be sure that wireless consumers and carriers can functionally implement the new legal requirements. But the Federal spam legislation ought to reflect the particular characteristics of the wireless technology and use this bill as a way to ensure that we have promulgated rules requiring a consumer opt-in for wireless e-mail messages so that the consumer has affirmatively said that they want these messages to come into their life. Otherwise, this device that is so valuable now to 170 million Americans would just be the single greatest nuisance ever invested.

Mr. Speaker, I rise in support of the compromise spam legislation that we bring to the House floor today.

Mr. Speaker, this legislation reflects a series of agreements between advocates for the two alternative House spam bills—one offered by Chairman TAUZIN, and the other offered by Ms. WILSON and Mr. GREEN of which I am an original cosponsor, as well as a series of compromises with our Senate counterparts. While not a perfect bill, I believe it merits support.

In addition, Mr. Speaker, this legislation now contains a modified version of the wireless spam amendment that I had offered for inclusion. The legislation preserves important authority of the FCC and FTC where it serves consumer interests. It also requires the FCC to initiate a rulemaking for wireless spam so that no loopholes are created but in a way to ensure that wireless consumers have greater protection than that accorded in the underlying bill.

As we attempt to tackle the issue of spam that is sent to our desktop computers, we must also recognize the millions of wireless consumers in the United States run the risk of being inundated with wireless spam. Unsolicited wireless text messages have plagued wireless users in Europe, South Korea, and Japan over the last few years as wireless companies in such countries have offered wireless messaging services. In Japan alone, NTT DoCoMo estimates that its wireless network processes some 800 million wireless spam messages a day. As cumbersome and annoying as spam to a desktop computer is, at least a consumer can turn off their computer and walk away. Wireless spam is even more intrusive because spam to wireless phones is the kind of spam that follows you wherever you go and according to U.S. wireless carriers, is already on the rise.

To prevent wireless spam from overwhelming the American wireless marketplace as it has networks in other countries, this legislation tasks the FCC to promulgate rules in order to put strong consumer protections on the books. In addition, the bill requires the FCC to consider certain provisions with an eye toward assessing them perhaps the unique capabilities or limitations of wireless devices. We must be sure that wireless consumers and carriers can functionally implement the legal requirements. Federal spam legislation ought to reflect the particular characteristics of wireless technology and use and this bill will allow the FCC to promulgate rules requiring a consumer "opt-in" for wireless email messages while examining the nature of a consumer's relationship with their wireless phone and service to take into account the unique service and technical characteristics that may warrant wireless-specific rules affecting consumer and carrier rights and obligations.

The wireless spam provision of the bill offers wireless consumers relief by requiring an "opt-in" for spam to wireless consumers. This reflects the fact that spam to a mobile phone is more intrusive to consumers and the fact that some wireless payment plans currently charge users for the amount of text messages they receive.

The provision would require "express prior authorization" from the consumer before an entity could send spam to their wireless device. My intent is that this "express prior authorization" be implemented in a way that a

request for "express prior authorization" is conspicuous and easily understood by consumers and that each entity seeking to send mobile service commercial messages pursuant to Section 14(b)(1) obtain such consumer authorization. In addition, the wireless spam provision requests that the FCC consider the ability of an initiator of spam to reasonably determine whether an electronic mail message is a mobile service commercial message. Obviously, as wireless service evolves, more and more consumers will receive Internet emails via their commercial mobile service provider's network and directly to their wireless device. If a person has an email address from their commercial mobile service provider and it can be readily identified as a wireless address, such as `name@verizonwireless.net` or `name@wireless.net` then the reasonable ability of a potential spammer to recognize that as such is relatively easy. Hopefully, commercial mobile service providers—and consumers—will see the benefit of having an email address that can be reasonably determined to be a wireless address, so that the prospect of massive amounts of spam to consumers over wireless networks can be thwarted and consumers can enjoy the benefits of entities needing their express prior authorization before sending them wireless spam.

Spam sent to desktop computer email address, and which is then forwarded over a wireless network to a wireless device, i.e., delivered "indirectly" from the initiator to the wireless device, would be treated by the rest of this bill and not by the wireless specific provisions we subject to an FCC rulemaking.

This legislation also represents an improvement in other areas over the Senate-passed bill. For example, the compromise doubles the damage caps in the Senate bill. It also eliminates the knowledge standards for the Federal Communications Commission (FCC), the Federal Trade Commission (FTC) and state Attorney General injunctive relief. The bill provides for rulemaking authority to clarify and tighten the definition of what constitutes a "commercial email." Requires that identifiers and a postal address must be on all commercial emails to desktop computers. Finally, the bill also shortens the time frame from which an "opt-out" request would become enforceable.

All of these represent important improvements over the Senate bill.

I want to commend Chairman TAUZIN, Ranking Member Mr. DINGELL for their excellent work in this area. I want to salute Representatives HEATHER WILSON and GENE GREEN for spearheading House spam efforts in this session as well as in the previous Congress as the lead sponsors of the House bill.

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

Mr. SENSENBRENNER. Mr. Speaker, I have no further requests for time from Committee on the Judiciary, and I yield the balance of my time to the gentleman from North Carolina (Mr. BURR).

Mr. BURR. Mr. Speaker, I ask unanimous consent to control the time of the gentleman from Louisiana (Mr. TAUZIN) as well as the time of the gentleman from Wisconsin (Mr. SENSENBRENNER).

The SPEAKER pro tempore (Mr. THORNBERRY). Is there objection to the request of the gentleman from North Carolina (Mr. BURR)?

There was no objection.

The SPEAKER pro tempore. The gentleman from North Carolina (Mr. BURR) has 5 minutes remaining, and the gentleman from Massachusetts (Mr. MARKEY) has 6 minutes remaining.

Mr. BURR. Mr. Speaker, I yield myself 2 minutes. Mr. Speaker, we are here today to get rid of unwanted sexually explicit e-mail, but we are also here to protect those individuals who want to use e-mail as a commercial tool in a responsible way based upon the rules, and the challenge for us was to design something that allowed commerce to take place but that got at the heart of what all of us wanted to do, and that is to get the smut off of our screen, to make sure that the ones that were unsolicited and that we did not want to see again, that we had the opportunity to get rid of them. And I am going to tell the Members it was tough, I think we would all agree, trying to find the right language, the right word in some cases, to make sure that the right penalty was in place but it did not go too far. And I think it is safe to say today that there is no single piece of legislation that will ultimately solve the spam problem.

It is my hope that this bill is an excellent first start. I believe that it is appropriate to praise the gentleman from Louisiana (Chairman TAUZIN) and the gentleman from Michigan (Mr. DINGELL), ranking member, and Gregg Rothschild and David Cavicke and many other committee staff and personal staffs that worked tirelessly to try to come up with a solution to the problem that we had. The FTC's own estimates estimate that 20 percent of all spam contains advertising of pornography. That is not counting the spam that we received that has deceptive content and fraudulent content.

Mr. Speaker, we are here today because we think we found the right blueprint. We think those businesses that are reputable can continue, and they can live within the framework, and they can live by the rules, and, hopefully, this will help to chase those that intended not to live by the rules out of the system and off our screen.

I want to praise once again both committees, the Committee on the Judiciary and the Committee on Energy and Commerce, the staffs and the members, and urge support for this bill.

Mr. MARKEY. Mr. Speaker, I yield 1 minute to the gentleman from Michigan (Mr. DINGELL).

Mr. DINGELL. Mr. Speaker, I thank the distinguished gentleman from Massachusetts for yielding me this time.

And I just want the attention of the gentleman from North Carolina (Mr. BURR). I want to pay tribute to him for the very honorable and splendid way in which he has worked with us to bring this matter to conclusion. Without his labors and those of the gentleman from Louisiana (Mr. TAUZIN), chairman of the Committee on Energy and Commerce, we would not be here talking about this matter. And I thank both

gentlemen, and I thank also Jonathan Cordone.

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

And I yield myself that time in order to conclude the debate for the Democratic side, and I would like to point out how important this bill is.

Congress many times acts in areas where most Americans say "How does that affect me?" This legislation will now affect every computer in the United States in the way in which it affects the user of that computer, and it will affect every user of a cell phone in the way that that cell phone is used or, to be more explicit, the way in which marketers abuse those phones and computers. So this is a great day, and the gentleman from New Mexico (Mrs. WILSON) and the gentleman from Texas (Mr. GREEN) did a great job in bringing it to our attention, and the gentleman from Louisiana (Chairman TAUZIN) and the gentleman from Michigan (Mr. DINGELL), in putting together an environment in which we can negotiate this bill out in a bipartisan fashion.

The litany of saints is long, and I mentioned many of them earlier. I would like to add the gentleman from Michigan (Mr. CONYERS), the ranking member of the Committee on the Judiciary. He and his staff contributed significantly to this legislation. To the gentleman from North Carolina (Mr. BURR), I want to congratulate him and his excellent work on this legislation. The consumers will be the beneficiary. I want to mention the gentleman from Silicon Valley, California (Ms. ESHO) for all of her wonderful work on this legislation. The gentleman from New Jersey (Mr. HOLT), who had a deep interest in the wireless aspects of this legislation, I think he deserves credit for what is happening here today. The gentleman from Louisiana (Chairman TAUZIN), David Cavicke did a great job, and I think I should mention Howard Waltzman as well on the chairman's staff for his excellent work; on the gentleman from Michigan's (Mr. UPTON) staff, Will Nordwind, who has been working on this for several months, as well with the chairman. And I would conclude by thanking my own staff, Colin Crowell, who throughout this year had a plan to include a wireless cell phone antispam provision in the legislation, and today we see the fruition of all of his excellent work, and I think that consumers will be the beneficiary for the generation ahead. So I conclude by complimenting the chairman.

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

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

In concluding, let me, first of all, again signal the extraordinary cooperation that exists between the Committee on the Judiciary and the Committee on Energy and Commerce as we conclude this debate and also to echo

thanks and congratulations the gentleman from Massachusetts (Mr. MARKEY) has extended to so many of our staff and the members who have worked on this.

This is a consumer protection piece of legislation. Very often when we come to these consumer protection-type pieces of legislation, we will see this extraordinary bipartisanship and this ability of committees that often have conflicting versions of bills work them out as we have today. This is a huge consumer protection piece of legislation.

And I want to say something that I hope all the Federal judges of America will pay attention to tonight very carefully. This legislation specifically authorizes the Federal Trade Commission to create a Do Not Spam Registry. No one should have any doubt about it. It is as clear, it is explicit. When this legislation passes the Congress and is signed into law, the FTC will explicitly have that authority, and a Do Not Spam Registry will be available in our future.

I want to particularly thank the gentleman from New Mexico (Mrs. WILSON), the gentleman from North Carolina (Mr. BURR), the gentleman from Texas (Mr. GREEN). Of all the members who have put in yeoman hours in time and effort, these three members of our committee have done an extraordinary job. And I particularly, again, want to single out the gentleman from Michigan (Mr. DINGELL) and the gentleman from Massachusetts (Mr. MARKEY) with, again, the bipartisan spirit in which we worked together when we can and do work together so well. This is a good example where America will benefit because we are legislating as Americans and not as party members as we often do on this floor. And I want to thank the gentleman, again, for that respect and that spirit of cooperation that he always extended to the chair and to the management of our committee affairs.

Again, Mr. Speaker, this is an important day for consumers in America. Very soon a Do Not Spam Registry will be available to them. They will be able to call and have their names put on that registry. People who refuse to pay attention to that registry and spam them regardless will be subject to severe penalties. People who fraudulently continue to spam without identifying who they are, when they are caught, will pay a big price. Attorney Generals and the FTC are given enforcement authority under this compromise, and I think we are affording Americans with a brand new tool to protect themselves against the entry of material they do not want in their homes whether it comes in through the computer, through the telephone, or via the mail. This is a great step forward, and I urge adoption of this bill.

Ms. ESHOO. Mr. Speaker, I support the conference report and thank the chairman and ranking member for their work in this effort. I'm particularly pleased that the serious short-

comings of the bill which I've raised at our committee have been addressed.

The problem of spam has become so prolific that by the end of this year half of all e-mails sent will be spam.

The numbers are staggering: 76 billion spam e-mails will be delivered in 2003; 50 percent of kids have received e-mails containing pornographic or sexually explicit information; and U.S. businesses will spend close to \$10 billion to fight spam this year.

And marketers have brazenly claimed that the success of the "Do Not Call List" will drive them to spam even more, costing U.S. businesses and consumers even more.

I sponsored legislation to curb the epidemic of spam and crafted the original proposal to empower the FTC to replicate the enormous success of the "Do Not Call List" by creating a "Cannot Spam List." I'm very pleased that a version of this measure has been included in the conference report, which I hope the FTC will implement soon after enactment of this bill.

I'm also pleased that the conference report strengthens some of the weaknesses of the Senate bill, especially by giving greater authority to states to enforce these laws.

This legislation does not end the entire problem of spam. I'll continue to fight for measures to prevent unauthorized and unwanted e-mail from flooding our inboxes and our computer networks. But this is a good start and important and I urge my colleagues to support it.

Mr. HOLT. Mr. Speaker, I rise in support of the anti-spam legislation before us, S. 877.

I am glad to see that Congress has finally taken definitive action on this issue. During my first term in Congress, I worked with my colleagues GENE GREEN and HEATHER WILSON, who have shown great leadership here, on anti-spam legislation that passed the House in 2000.

Today we have before us legislation to help address the mounting problem of unsolicited e-mail advertising, or spam, which has become perhaps the biggest nuisance of the Information Age and a drain on our economy.

I am particularly pleased that this legislation includes a provision intended to combat a related problem that has gotten out of hand in some countries and is growing ever worse in the United States—spam sent to wireless phones through text messaging.

As many of my colleagues know, I introduced legislation intended to draw attention to this issue—the Wireless Telephone Spam Protection Act. This bill was intended to launch what could be called a preemptive attack against wireless spam before it spins out of control in the United States. Congress too often acts once the fire is already lit. This time, we can put the fire out before it gets out of control.

The Japanese are already fighting off a tsunami of cell phone spam. On one recent day, the 38 million customers of the largest Japanese wireless company, NTT DoCoMo, received 150 million pieces of spam. Even today, after passage of anti-spam laws in Japan, DoCoMo's subscribers still receive up to 30 million wireless spam messages each day. This has caused millions of Japanese wireless phone users to simply stop using their cell phone service.

So far, U.S. cell phone users have been largely spared this torrent of annoying, un-

wanted messages. I presume this is because a lot of telemarketers don't believe there are enough text-capable cell phones in the country. Most new phones are text capable, however, and the number of text messages sent in this country has been rising rapidly, quadrupling from 250 million messages sent in December 2001 to 1 billion messages sent in December 2002. Seventeen percent of cellular customers, about 23 million people, currently use text messaging—including 45 percent of cell phone users in the lucrative 18-to-25-year-old category. Direct marketers are already beginning to salivate.

That is why I am glad to see that this legislation includes a provision instructing the Federal Trade Commission to promulgate an opt-in rule for wireless spam. I would like to thank Mr. MARKEY for his work on this issue, and I would like to salute all of those who put this legislation together. It is by no means cure-all, but it is certainly a good first step towards ending the onslaught of e-mail spam and the tsunami of wireless spam. I urge my colleagues to support this bill.

Mr. STUPAK. Mr. Speaker, for several Congresses now we have had hearings and mark-ups in the Energy and Commerce Committee on the nuisance of spam, but no progress has been made. I am pleased that a bill has finally come forward that looks headed for passage into law.

Through all this time, the flood of unsolicited e-mails has only grown, ISPs have become more and more overwhelmed, and consumers

more aggravated. My bill will come as a welcome relief to many who are fed up with opening their e-mail accounts only have to unwanted commercial e-mails clogging up their Internet mailboxes.

Consumers have to waste time deleting numerous spam e-mails, and even worse, if they do unsuspectingly open one of these e-mails, they are often faced with offensive pornography.

I commend the members of the Judiciary and Energy and Commerce Committees for their ongoing efforts to address this problem, and I am pleased to support this bill.

I do believe that the bill falls short in one area, in that it does not provide a private right of action for individual consumers to seek their own remedies. But this legislation does much to strengthen enforcement, provide protection from harmful pornographic e-mails, and to set up a Do Not Spam Registry, which I can only guess will be as popular as the Do Not Call Registry.

I hope that this bill will put control over Internet mailboxes back in the hands of consumers, so that they can choose to receive e-mails that they want, and to get rid of e-mails that they do not.

And to those businesses and individuals that violate these provisions and send out spam illegally, this bill will provide the Federal Trade Commission, state attorney generals, and Internet Service Providers with the tools to crack down on these violators.

As the House attempts to wrap up its work for the session, there have been several bills coming to the floor that I do not believe have merit. This bill, however, shows that when we want to, Congress can truly act for the public benefit.

Mr. STEARNS. Mr. Speaker, I am pleased to join Chairman TAUZIN, Chairman SENSENBRENNER, Messrs. DINGELL and BURR, and

Mrs. WILSON in supporting a good consumer protection bill that I hope will help us, as consumers, fight the scourge that is spam.

No one disputes the great utility of e-mail, the fact that it has brought great efficiency and productivity gains, not only to our professional lives but also our personal lives. Nonetheless, our daily routine of scouring through and reviewing our e-mail also tells us that e-mail as a critical communications medium is under assault from unwanted e-mail—most peddling goods or services ranging from the real to the absurd. I do not have a problem with e-marketing per se, after all, our consumer based economy is highly dependent on marketing. However, e-mail communications make accountability more difficult. Therefore, unscrupulous people use it to advance fraudulent and deceptive acts and even good commercial actors are tempted to take advantage of this lack of accountability.

Effective and narrowly tailored legislation, like the one before us today, can help bring greater accountability to e-mail solicitations. That greater accountability is achieved by making sure that fraud and deception is prosecuted and subjected to severe penalties.

Legislation is only part of the solution, and in my view a smaller part. Rather, technology, consumer education, and industry cooperation, in my view, are the key tools in combating spam and injecting real and effective accountability. Finally, combating spam requires international cooperation. I think my bi-partisan bill, H.R. 3143, which strengthens the Federal Trade Commission's ability to address the growing problem of transnational fraud, will go a long way in fighting spam that is not home grown.

Mr. TAUZIN. 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 Louisiana (Mr. TAUZIN) that the House suspend the rules and pass the Senate bill, S. 877, as amended.

The question was taken. In the opinion of the Chair, two-thirds of those present have voted in the affirmative.

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

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

CONFERENCE REPORT ON H.R. 2622, FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003

Mr. OXLEY (during consideration of H. Res. 458) submitted the following conference report and statement on the bill (H.R. 2622) to amend the Fair Credit Reporting Act, to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, make improvements in the use of, and consumer access to, credit information, and for other purposes:

CONFERENCE REPORT (H. REPT. 108-396)
The committee of conference on the disagreeing votes of the two Houses on the

amendment of the Senate to the bill (H.R. 2622), to amend the Fair Credit Reporting Act, to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, make improvements in the use of, and consumer access to, credit information, and for other purposes, having met, after full and free conference, have agreed to recommend and do recommend to their respective Houses as follows:

That the House recede from its disagreement to the amendment of the Senate and agree to the same with an amendment as follows:

In lieu of the matter proposed to be inserted by the Senate amendment, insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) *SHORT TITLE.*- This Act may be cited as the "Fair and Accurate Credit Transactions Act of 2003".

(b) *TABLE OF CONTENTS.*- The table of contents for this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Definitions.
- Sec. 3. Effective dates.

TITLE I.—IDENTITY THEFT PREVENTION AND CREDIT HISTORY RESTORATION

Subtitle A.—Identity Theft Prevention

- Sec. 111. Amendment to definitions.
- Sec. 112. Fraud alerts and active duty alerts.
- Sec. 113. Truncation of credit card and debit card account numbers.
- Sec. 114. Establishment of procedures for the identification of possible instances of identity theft.
- Sec. 115. Authority to truncate social security numbers.

Subtitle B.—Protection and Restoration of Identity Theft

- Sec. 151. Summary of rights of identity theft victims.
- Sec. 152. Blocking of information resulting from identity theft.
- Sec. 153. Coordination of identity theft complaint investigations.
- Sec. 154. Prevention of repopulation of consumer reports.
- Sec. 155. Notice by debt collectors with respect to fraudulent information.
- Sec. 156. Statute of limitations.
- Sec. 157. Study on the use of technology to combat identity theft.

TITLE II.—IMPROVEMENTS IN USE OF AND CONSUMER ACCESS TO CREDIT INFORMATION

- Sec. 211. Free consumer reports.
- Sec. 212. Disclosure of credit scores.
- Sec. 213. Enhanced disclosure of the means available to opt out of prescreened lists.

TITLE III.—ENHANCING THE ACCURACY OF CONSUMER REPORT INFORMATION

- Sec. 311. Risk-based pricing notice.
- Sec. 312. Procedures to enhance the accuracy and integrity of information furnished to consumer reporting agencies.
- Sec. 313. FTC and consumer reporting agency action concerning complaints.
- Sec. 314. Improved disclosure of the results of re-investigation.
- Sec. 315. Reconciling addresses.
- Sec. 316. Notice of dispute through reseller.

TITLE IV.—LIMITING THE USE AND SHARING OF MEDICAL INFORMATION IN THE FINANCIAL SYSTEM

Sec. 411. Protection of medical information in the financial system.

Sec. 412. Confidentiality of medical contact information in consumer reports.

TITLE V.—FINANCIAL LITERACY AND EDUCATION IMPROVEMENT

- Sec. 511. Short title.
- Sec. 512. Definitions.
- Sec. 513. Establishment of Financial Literacy and Education Commission.
- Sec. 514. Duties of the Commission.
- Sec. 515. Powers of the Commission.
- Sec. 516. Commission personnel matters.
- Sec. 517. Studies by the Comptroller General.
- Sec. 518. The national public service multimedia campaign to enhance the state of financial literacy.
- Sec. 519. Authorization of appropriations.

TITLE VI.—PROTECTING EMPLOYEE MISCONDUCT INVESTIGATIONS

Sec. 611. Certain employee investigation communications excluded from definition of consumer report.

TITLE VII.—RELATION TO STATE LAWS

Sec. 711. Relation to State laws.

TITLE VIII.—MISCELLANEOUS

Sec. 811. Clerical amendments.

SEC. 2. DEFINITIONS.

As used in this Act—

(1) the term "Board" means the Board of Governors of the Federal Reserve System;

(2) the term "Commission", other than as used in title V, means the Federal Trade Commission;

(3) the terms "consumer", "consumer report", "consumer reporting agency", "creditor", "Federal banking agencies", and "financial institution" have the same meanings as in section 603 of the Fair Credit Reporting Act, as amended by this Act; and

(4) the term "affiliates" means persons that are related by common ownership or affiliated by corporate control.

SEC. 3. EFFECTIVE DATES.

Except as otherwise specifically provided in this Act and the amendments made by this Act—

(1) before the end of the 2-month period beginning on the date of enactment of this Act, the Board and the Commission shall jointly prescribe regulations in final form establishing effective dates for each provision of this Act; and

(2) the regulations prescribed under paragraph (1) shall establish effective dates that are as early as possible, while allowing a reasonable time for the implementation of the provisions of this Act, but in no case shall any such effective date be later than 10 months after the date of issuance of such regulations in final form.

TITLE I.—IDENTITY THEFT PREVENTION AND CREDIT HISTORY RESTORATION

Subtitle A.—Identity Theft Prevention

SEC. 111. AMENDMENT TO DEFINITIONS.

Section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a) is amended by adding at the end the following:

"(q) **DEFINITIONS RELATING TO FRAUD ALERTS.**—

"(1) **ACTIVE DUTY MILITARY CONSUMER.**— The term "active duty military consumer" means a consumer in military service who—

"(A) is on active duty (as defined in section 101(d)(1) of title 10, United States Code) or is a reservist performing duty under a call or order to active duty under a provision of law referred to in section 101(a)(13) of title 10, United States Code; and

"(B) is assigned to service away from the usual duty station of the consumer.

DOCUMENT NO. 13

