

HEINONLINE

Citation: 1 Controlling the Assault of Non-Solicited Pornography
Marketing CAN-SPAM Act of 2003 A Legislative History
H. Manz ed. H12854 2004

Content downloaded/printed from
HeinOnline (<http://heinonline.org>)
Mon Apr 22 11:24:28 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.

Quinn Stark Waxman
Rohrabacher Thornberry Wexler
Schiff Vitter Young (AK)

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE
The SPEAKER pro tempore (Mr. LATOURETTE)(during the vote). Members are advised there are 2 minutes remaining in this vote.

□ 1704

Messrs. FRANK of Massachusetts, DAVIS of Illinois, and HALL changed their vote from "yea" to "nay."

Messrs. OSBORNE, RYUN of Kansas, GREENWOOD, AKIN, BEAUPREZ, and TANCREDO, and Ms. HART changed their vote from "nay" to "yea."

So the motion to table was agreed to. The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

Stated against:

Mr. FILNER, Mr. Speaker, on rollcall No. 677, due to urgent constituent support commitments in my congressional district, I missed the vote. Had I been present, I would have voted "no."

PERSONAL EXPLANATION

Mr. PASCRELL, Mr. Speaker, the conference report for H.R. 2673 allows disastrous overtime regulations to go through, bows to pressure on FCC media ownership regulations, contains inadequate funding for the manufacturing extension partnership, and includes a flawed public school vouchers program. I have opposed all of these provisions in past votes. While I have strong concerns about these and other provisions contained in and left out of this omnibus appropriations bill, had I been in attendance, I would have cast an "aye" vote on rollcall No. 676 in support of the many important programs this bill funds.

I would have voted "no" on rollcall No. 677, the motion to table the Democratic Leader's Privileged Resolution.

PERSONAL EXPLANATION

Mr. BURTON of Indiana, Mr. Speaker, due to official business outside the Washington, DC, area, I was unable to be present during rollcall votes 673-677. Had I been here I would have voted "yea" for rollcall votes 673-677.

APPOINTMENT OF COMMITTEE OF TWO MEMBERS TO INFORM THE PRESIDENT THAT THE HOUSE HAS COMPLETED ITS BUSINESS OF THE SESSION

Mr. DELAY, Mr. Speaker, I offer a privileged resolution (H. Res. 476) and ask for its immediate consideration.

The Clerk read the resolution, as follows:

H. Res. 476

Resolved, That a committee of two Members of the House be appointed to wait upon the President of the United States and inform him that the House of Representatives has completed its business of the session and is ready to adjourn, unless the President has some other communication to make to them.

The resolution was agreed to.

A motion to reconsider was laid on the table.

The SPEAKER pro tempore. Pursuant to House Resolution 476, the Chair

appoints the following Members of the House to the Committee to Notify the President:

The gentleman from Texas (Mr. DELAY);
the gentlewoman from California (Ms. PELOSI).

AUTHORIZING THE SPEAKER, MAJORITY LEADER, AND MINORITY LEADER TO ACCEPT RESIGNATIONS AND TO MAKE APPOINTMENTS AUTHORIZED BY LAW OR BY THE HOUSE FOR THE REMAINDER OF THE 108TH CONGRESS

Mr. DELAY, Mr. Speaker, I ask unanimous consent that for the remainder of the 108th Congress, the Speaker, the Majority Leader, and the Minority Leader be authorized to accept resignations and to make appointments authorized by law or by the House.

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

There was no objection.

GRANTING MEMBERS OF THE HOUSE PRIVILEGE TO EXTEND AND REVISE REMARKS IN CONGRESSIONAL RECORD UNTIL LAST EDITION IS PUBLISHED

Mr. DELAY, Mr. Speaker, I ask unanimous consent that Members may have until publication of the last edition of the CONGRESSIONAL RECORD authorized for the first session of the 108th Congress by the Joint Committee on Printing to revise and extend their remarks and to include brief, related extraneous material on any matter occurring before the adjournment of the first session sine die.

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

There was no objection.

REMOVAL OF NAME OF MEMBER AS COSPONSOR OF H.R. 3507

Ms. PELOSI, Mr. Speaker, I ask unanimous consent to have my name removed as a cosponsor of H.R. 3507.

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

There was no objection.

REMOVAL OF NAME OF MEMBER AS COSPONSOR OF H. Res. 462

Mr. TERRY, Mr. Speaker, I ask unanimous consent to have my name removed as a cosponsor of H. Res. 462.

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

There was no objection.

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

Mr. TAUZIN, Mr. Speaker, I ask unanimous consent to take from the Speaker's table the Senate bill (S. 877) to regulate interstate commerce by im-

posing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet, with a Senate amendment to the House amendment thereto, and concur in the Senate amendment to the House amendment.

The Clerk read the title of the Senate bill.

The Clerk read the Senate amendment to the House amendment, as follows:

Senate amendment to House amendment: In lieu of the matter proposed to be inserted by the House amendment to the text of the bill, insert:

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 non-commercial, 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 messages' 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 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 one 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 one 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", when used with respect to a commercial electronic mail message, 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 throughout the message 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 five or more electronic mail accounts or online user accounts or two 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 3 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 one 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(c) of this title.

"(2) MATERIALLY.—For purposes of paragraphs (3) and (4) of subsection (a), header information or registration information is materially falsified 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 994(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

(ii) 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), as 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 message 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 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 mailing lists bearing the electronic mail address of the recipient for any purpose other than compliance with this Act or other provision of law.

(B) **SUBSEQUENT AFFIRMATIVE CONSENT.**—A prohibition in 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 message if the recipient has given prior affirmative consent to receipt of the message.

(6) **MATERIALLY.**—For purposes of paragraph (1), the term "materially", when used with respect to false or misleading header information, includes the alteration or concealment of header information 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 a 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 regulation, 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.

(5) **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 the 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.**—Except as provided in section 7(f)(8), 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 (a), (b), (c), or (d) of this section to enforce compliance, through an order to cease and desist or an injunction, with section 5(a)(1)(C), section 5(a)(2), clause (ii), (iii), or (iv) of section 5(a)(4)(A), section 5(b)(1)(A), or section 5(b)(3), 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), who violates section 5(d), or who en-

gages 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 (3).

(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)(1)(C), section 5(a)(2), clause (ii), (iii), or (iv) of section 5(a)(4)(A), section 5(b)(1)(A), or section 5(b)(3).

(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 reasonable practices and procedures designed to effectively prevent such violations; or

(ii) the violation occurred despite commercially reasonable efforts to maintain compliance the practices and procedures to which reference is made in clause (i).

(4) ATTORNEY FEES.—In the case of any successful action under paragraph (1), the court, in its discretion, may award the costs of the action and reasonable attorney fees to the State.

(5) 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.

(6) 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.

(7) 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.

(8) 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.

(9) REQUISITE SCIENTER FOR CERTAIN CIVIL ACTIONS.—Except as provided in section 5(a)(1)(C), section 5(a)(2), clause (ii), (iii), or (iv) of section 5(a)(4)(A), section 5(b)(1)(A), or section 5(b)(3), 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.

(6) 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)(1), 5(b), or 5(d), or a pattern or practice that violates 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) the 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) up to \$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 designed to effectively prevent such violations; or

(ii) the violation occurred despite commercially reasonable efforts to maintain compliance with the practices and procedures to which reference is made in clause (i).

(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.**—(i) Nothing in this Act shall be construed to impair the enforcement of section 223 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. 8102).

(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 Federal Communications Commission, in promulgating 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 to the sender, 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 sender;

(3) take into consideration, in determining whether to subject providers of commercial mobile 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 from the provider—

(A) at the time of subscribing to such service; and

(B) in any billing mechanism; and

(4) determine how a sender 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 a sender of a commercial electronic mail message to reasonably determine that the 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 is transmitted directly to a wireless device that 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.

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.

Mr. TAUZIN (during the reading).
Mr. Speaker, I ask unanimous consent that the Senate amendment to the House amendment be considered as read and printed in the RECORD.

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

There was no objection.

Mr. SENSENBRENNER. Mr. Speaker, I rise in support of the bill S. 877, as returned by the

Senate with technical changes. I urge my colleagues to pass once more and send it on to the President.

The House of Representatives passed this legislation previously on November 21, 2003. The changes made herein to the language are not substantive departures from what previously passed the House, but are merely necessary to correct minor errors in the drafting to accurately reflect the will of Congress.

Taking the final legislative step today necessary to put into law a unified federal approach to the problem of unsolicited commercial email or "spam" represents an important moment in protecting children and the "inboxes" of millions of Americans.

The bill provides consumers with more information and choices to stop receiving all forms of unwanted commercial email and provides federal and state officials and providers on Internet access with the tools to go after spammers. As I noted previously, the criminal provisions contained in this legislation are central to its purpose. In order to provide a credible deterrent against spamming, this legislation establishes enhanced criminal penalties for predatory spamming and provides law enforcement personnel far more authority to prosecute spammers whose electronic presence can shift with a keystroke.

I believe this legislation will take a bite out of spam and spammers, and it will have some effect in reducing the type and amount of spam that online users deal with today. However, it is not a panacea. In the midst of speaking about the positive things that S. 877 does, it is important to put all concerned on notice that no legislation, no matter how severe, can stop spam entirely. The most hard core group of problematic spammers already operate sometimes in defiance of multiple laws and it will take time and effort to track down even those within the reach of U.S. jurisdiction. Furthermore, policy makers should be wary of any "soundbite" legislative or regulatory approach to this problem that promises to end all spam—because such an approach would surely have drastic consequences for free speech and the legitimate forms of e-mail that consumers want and use.

Consumers and their Internet service providers can do far more to protect the nation's inboxes from unsolicited e-mail than any law that can be passed here or in state capitals. Already, consumers who take full advantage of existing firewalls, blocking software, and "challenge/response" protocols enjoy a dramatically reduced amount of spam—and many of these options are free or included in the package of services offered by their Internet access provider.

Ultimately, spam will be stopped by a combination of new technology, consumer awareness, ISP filtering, and trusted sender systems for legitimate senders of commercial e-mail—with laws and regulation merely setting the outer boundaries of illegitimate e-mail practices. In the interim, this legislation will help fill the gap. I encourage those plagued by unwanted e-mail today to take advantage of the practices and technologies that are proven to reduce spam as well as the remedies provided under this law and others.

Mr. Speaker, I am pleased that the House today is sending the final version of this important anti-fraud and consumer protection measure on to the President, and the President has indicated he will sign the bill. I urge my colleagues to support the legislation.

Mr. MARKEY. Mr. Speaker, I rise in support of S. 877, spam legislation that we bring to the House Floor today in a final version that incorporates technical and other changes since the House sent to the Senate a compromise bill on November 21.

Mr. Speaker, as I noted in remarks back in November, 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.

Mr. Speaker, this legislation now contains the Markey amendment on wireless spam, which originated in the House amendments to the Senate-passed bill. The reason I offered this amendment for inclusion in the House-passed bill is that I wanted wireless consumers to have greater protection than that which was accorded in the version of S. 877 which the Senate passed previously.

Indeed, during the summer the Energy and Commerce Committee held a hearing on spam at which I raised the prospect of wireless spam and the likelihood that it was a problem wireless consumers were beginning to see. At that time, neither the Tauzin-Burr spam bill, nor the Wilson-Green spam bill, continued wireless specific provisions to address this issue head-on.

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. According to published reports that came to our attention as we were deliberating upon the spam issue, NTT DoCoMo estimated 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.

For this reason, in order to safeguard consumer privacy in a way that reflects the more intrusive nature of wireless spam to the user than spam is to a desktop computer, which is immobile and for which the user may pay some type of "per message" fee, the bill tasks the FCC with tackling this issue now, before it overwhelms users and network operators alike. The same type of rules that are applicable to commercial e-mail messages sent to personal computers will clearly also apply to those sent to wireless devices, including mobile phones, and the general provisions of the bill would apply to wireless messages as they would to similar messages sent to a desktop computer. Section 14 of the bill builds upon this legislative foundation and puts in place additional protections and modifications. It requires an FCC rulemaking to assess and put in place additional consumer protections. The bill doesn't needlessly or unduly burden wireline network operators—and wireless carriers should not see such burdens implemented as part of Section 14 to the extent to which they are acting as carriers. Of course, these same wireless carriers may also be senders of spam themselves, and the bill

spells out how such messages should be dealt with and includes the FCC proceeding in Section 14 to address issues particular to wireless services.

Again, Mr. Speaker, 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 certain wireless e-mail messages. In addition, this proceeding permits the FCC to examine the nature of a consumer's relationship with their wireless phone and service to take into account the potentially unique technical characteristics which may warrant wireless-specific rules.

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 e-mails via their commercial mobile service provider's network and directly to their wireless device. If a person has an e-mail 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 e-mail 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 a desktop computer e-mail 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 additional Section 14 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 e-mail." Requires that identifiers and a postal address must be on all commercial e-mails 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 and Ranking Member 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.

I yield back the balance of my time. The SPEAKER pro tempore. Is there objection to the original request of the gentleman from Louisiana?

There was no objection.

A motion to reconsider was laid on the table.

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 on S. 877.

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

There was no objection.

DEFENSE PRODUCTION ACT REAUTHORIZATION OF 2003

Mr. NEY. Mr. Speaker, I ask unanimous consent to take from the Speaker's table the Senate bill (S. 1680), to reauthorize the Defense Production Act of 1950, and for other purposes, with a Senate amendment to the House amendment thereto, and concur in the Senate amendment to the House amendment.

The Clerk read the title of the Senate bill.

The Clerk read the Senate amendment to the House amendment, as follows:

Senate amendment to House amendment: Page 6, strike line 1 and all that follows over to and including line 2 on page 7, of the House engrossed amendment, and insert:

SEC. 7. REPORT ON IMPACT OF OFFSETS ON DOMESTIC CONTRACTORS AND LOWER TIER SUBCONTRACTORS.

(a) EXAMINATION OF IMPACT REQUIRED.—

(1) *IN GENERAL.*—As part of the annual report required under section 309(a) of the Defense Production Act of 1950 (50 U.S.C. App. 2099(a)), the Secretary of Commerce (in this section referred to as the "Secretary") shall—

(A) detail the number of foreign contracts involving domestic contractors that use offsets, industrial participation agreements, or similar arrangements during the preceding 5-year period;

(B) calculate the aggregate, median, and mean values of the contracts and the offsets, industrial participation agreements, and similar arrangements during the preceding 5-year period; and

(C) describe the impact of international or foreign sales of United States defense products and related offsets, industrial participation agreements, and similar arrangements on domestic prime contractors and, to the extent practicable, the first 3 tiers of domestic contractors and subcontractors during the preceding 5-year period in terms of domestic employment, including any job losses, on an annual basis.

(2) *USE OF INTERNAL DOCUMENTS.*—To the extent that the Department of Commerce is already in possession of relevant data, the Department shall use internal documents or existing departmental records to carry out paragraph (1).

(3) INFORMATION FROM NON-FEDERAL ENTITIES.—

(A) *EXISTING INFORMATION.*—In carrying out paragraph (1), the Secretary shall only require a non-Federal entity to provide information that is available through the existing data collection and reporting systems of that non-Federal entity.

(B) *FORMAT.*—The Secretary may require a non-Federal entity to provide information to the Secretary in the same form that is already provided to a foreign government in fulfilling an offset arrangement, industrial participation agreement, or similar arrangement.

(b) REPORT.—

(1) *IN GENERAL.*—Before the end of the 8-month period beginning on the date of enactment of this Act, the Secretary shall submit to Congress a report containing the findings and conclusions of the Secretary with regard to the examination made pursuant to subsection (a).

(2) *COPIES OF REPORT.*—The Secretary shall also transmit copies of the report prepared under paragraph (1) to the United States Trade Representative and the interagency team established pursuant to section 123(c) of the Defense Production Act Amendments of 1992 (50 U.S.C. App. 2099 note).

(c) *RESPONSIBILITIES REGARDING CONSULTATION WITH FOREIGN NATIONS.*—Section 123(c) of the Defense Production Act Amendments of 1992 (50 U.S.C. App. 2099 note) is amended to read as follows:

"(i) NEGOTIATIONS.—

"(I) INTERAGENCY TEAM.—

"(A) *IN GENERAL.*—It is the policy of Congress that the President shall designate a chairman of an interagency team comprised of the Secretary of Commerce, Secretary of Defense, United States Trade Representative, Secretary of Labor, and Secretary of State to consult with foreign nations on limiting the adverse effects of offsets in defense procurement without damaging the economy or the defense industrial base of the United States or United States defense production or defense preparedness.

"(B) *MEETINGS.*—The President shall direct the interagency team to meet on a quarterly basis.

"(C) *REPORTS.*—The President shall direct the interagency team to submit to Congress an annual report, to be included as part of the report required under section 309(a) of the Defense Production Act of 1950 (50 U.S.C. App. 2099(a)), that describes the results of the consultations of the interagency team under subparagraph (A) and the meetings of the Interagency team under subparagraph (B).

"(2) *RECOMMENDATIONS FOR MODIFICATIONS.*—The interagency team shall submit to the President any recommendations for modifications of any existing or proposed memorandum of understanding between officials acting on behalf of the United States and 1 or more foreign countries (or any instrumentality of a foreign country) relating to—

"(A) research, development, or production of defense equipment; or

"(B) the reciprocal procurement of defense items."

Mr. NEY (during the reading). Mr. Speaker, I ask unanimous consent that the Senate amendment to the House amendment be considered as read and printed in the RECORD.

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

There was no objection.

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

Mr. CARDIN. Mr. Speaker, reserving the right to object, because I believe we are getting near the end of the business of this session of Congress, and at least on this side, we are not aware of whether the majority will allow unanimous consent requests in regard to the unemployment compensation extensions.

As my colleagues know, at the end of this month, we will expire the Federal Unemployment Compensation Program, and 80,000 to 90,000 individuals a week will exhaust their State unemployment benefits and will not be entitled to any Federal relief.

So I was wondering if the gentleman could just advise us as to whether the majority is prepared to allow unanimous consent requests, since there are no further recorded votes, I believe, anticipated today, so that we could at least bring up the extension of the unemployment compensation benefits to deal with the people who cannot find employment.

Mr. NEY. Mr. Speaker, will the gentleman yield?

Mr. CARDIN. I yield to the gentleman from Ohio.

Mr. NEY. Mr. Speaker, on this particular issue I am actually standing in for the gentleman from Ohio (Chairman OXLEY) on this particular unanimous consent bill. As far as the rest, that goes above my pay grade, but I am sure that our side will be more than happy to talk to your side.

Mr. OXLEY. Mr. Speaker, I rise in strong support of S. 1680, the Defense Production Act Reauthorization of 2003, and urge its adoption. The bill before the House is largely the same as H.R. 1280, and passed last spring by the Committee on Financial Services, and is the result of broad bipartisan and bicameral efforts to reauthorize and update this important Act.

Mr. Speaker, when the House acts today to send the bill to the President, it will be completing Congressional action that should have taken place no later than the end of September. The authorities in this Act are too important for the Nation to have been without them for the nine weeks.

That said, Mr. Speaker, what is before the House today is a very good product. First and foremost, it reauthorizes the Defense Production Act for five years. This is important for two reasons: Firstly, as the nation faces the uncertain times ahead, it will be important for the President to have the authorities in the Act, and secondly, because it will give Congress an opportunity to consider some much-needed modernization of the DPA decoupled from reauthorization cycle. It is my intent to ask the President to take the next year to ponder what sorts of modernization of the DPA is necessary, with the idea that any action on those or other recommendations would take place in the first session of the next Congress.

The bill we are considering today also adds as a specific goal of the DPA the protection of the nation's critical infrastructure. Given the increasing dependence of the nation's defense, financial services and in fact the fabric of our daily lives on our critical infrastructure, I believe this addition is both wise and important.

Finally, in addition to some other minor additions, the bill before us increases on a one-time basis the funding ceiling for a program to enhance the nation's ability to produce radiation-hardened electronics for use in, for example, defense satellites. This program is an example of one of the most important aspects of the DPA: creating a U.S. defense production capability where none now exists.

Most important of all of these, Mr. Speaker, is the reauthorization itself. The DPA is the tool that the President uses to meet a specific national security need—protective gear for our troops overseas, or specialized communications equipment—should we have a shortfall in

DOCUMENT NO. 17

