Good news comes not one thing at a time but two things and maybe three at a time, and the two pieces of great news are before us today. Let us hope there is more to come because, clearly, we are on the path upward.

I yield the floor.

CAN-SPAM ACT OF 2003

Mr. BURNS. Mr. President, as my good friend from New Mexico was pointing out some of the good news, I have some more. I ask that the Chair lay before the Senate a message from the House on S. 877.

The PRESIDING OFFICER laid before the Senate the following message:

S. 877

Resolved, That the bill from the Senate (S. 877) entitled ''An Act to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet'', do pass with the following amendment:

Strike out all after the enacting clause and 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 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 note).

(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 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 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 mailing 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 not 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 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.

(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.

(g) 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 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. 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.

Mr. BURNS. Mr. President, I ask unanimous consent that the Senate concur in the House amendment with the substitute amendment from Senator BURNS, the motion to reconsider be laid upon the table, with no intervening action or debate, and that any statements relating to the bill be printed in the RECORD.

The PRESIDING OFFICER (Mr. DOMENICI). Without objection, it is so ordered.

The amendment (No. 2219) was agreed to.

(The amendment is printed in today's RECORD under ''Text of Amendments.'')

Mr. BURNS. Mr. President, this is a good day, not only for me personally but many of us who serve in this Senate, especially my friend from Oregon whom I see across the aisle.

It has been 4 years, working on this legislation. This is the CAN–SPAM bill—everybody is pretty familiar with it—which we hope will stem the tide of junk mail that is flooding our Nation's inboxes and our e-mail.

I specifically thank my colleague Senator WYDEN from Oregon who is coauthor of this bill. He has been working tirelessly on this for years—as long as I have. Thanks to the discussions over the past few days, many already strong proconsumer provisions in CAN–SPAM have been enhanced. Those negotiations have been ongoing and, in some cases, have been rather tense. The bill the Senate considers today contains substantial statutory damages for spammers and additional notice requirements on commercial e-mail.

The character of the Congress is not always proactive; it is always reactive, it seems. That is the nature of the political landscape in which we find ourselves. We do not get too excited about doing anything until the folks at home get excited, or enough of them, that they form a critical mass for us to take action.

I congratulate Senator WYDEN. We serve together on the Commerce Committee. We were approached about doing something about the Internet and what is coming down on our computers and is found in our mailboxes on the Internet. We saw, 4 years ago, that this was going to become a problem. It was not just the idea of the Senator who stands before you now to do something about unwanted e-mail 4 years ago. There were more Senators around here who had the same vision, that as this industry grows, a problem will also grow with it. And that is what happened.

The extent of bipartisan cooperation on this issue is no surprise, given the deluge of spam consumers face in their inboxes every day. The costs to businesses and individuals is escalating and wide ranging. Businesses lose money when employees take more and more time to wade through their e-mail. Servers all over the country have difficulty blocking spam, clearing their machines so they can operate while spammers work to find more and more ways to circumvent the latest software server or individual blocking systems.

In my State of Montana, spam is really horrible, as it is in all rural areas across the United States. We have vast distances in Montana. Many of my constituents are forced to pay long distance charges on their time on the Internet. It is not the only State that has to do that. You will find that in the majority of rural areas, in all our States. Spam makes it nearly impossible for rural America to realize the tremendous economic and educational benefits of the online era.

This bill empowers consumers and grants additional enforcement to the Federal Trade Commission to take action against spammers. It also allows the States' attorneys general to do the same. The bill requires the senders of commercial e-mail to include a clear opt-out mechanism to allow consumers to be removed from the mass e-mail lists. This opt-out must also be clearly described in the e-mail itself, so users of e-mail are not forced to sift through pages and pages of legalese to determine where they can stop the unwanted mail. Senders of commercial e-mail must also provide a valid physical postal address, so they are not able to hide their identities. Finally, e-mail marketers must include a notice that the e-mail is advertising.

Simply put, the CAN–SPAM bill finally gives consumers a measure of control over their inboxes.

In cases where e-mail marketers don't comply with the CAN–SPAM bill, the penalties are very severe. For this part of the bill we have many people to thank. Spammers are actually on the hook for damages up to $250 per spam e-mail with a cap of $2 million. That gets my attention right there. This already high penalty can be tripled if particularly unethical methods are used, such as a computer hijacking to send spam by taking control of computers of legitimate users without their knowledge, and for harvesting addresses from legitimate Web sites to send spam. For criminal spammers who try to hide their identities by using false header information, damages are not capped. In other words, they can go as high, those damages can go as high as the market would stand. It also includes enhanced enforcement authority of the FCC to close possible loopholes for spammers and to keep up with the technological developments.

Let's face it, technology moves at the speed of light. Granting the Commission the ability to keep pace with new techniques of spammers is essential because it has become clear, in recent years anyway, that these criminals are growing increasingly sophisticated in their methods.

So the passage of this bill today will help stem the tide of the toxic sea of

spam. Clearly, consumers have been demanding control over their e-mail inboxes, and the passage of the CAN–SPAM today will give those consumers a key victory in the battle against criminal spammers.

Again, I thank my good friend with whom I served on the Commerce Committee, Senator WYDEN of Oregon, who has absolutely been a knight in shining armor in negotiations and working this through the Congress. Also on the floor is Senator SCHUMER of New York. Senator SCHUMER has offered many positive provisions in this bill. We have had a great time debating that. But nonetheless, his contribution is clearly in this bill and we appreciate his work. Of course, when I say it is a bipartisan effort, that is usually the way we get legislation passed around here, legislation that has any kind of future at all.

I thank them both. It gives me great pleasure to yield the floor for my friend from the great State of Oregon, Senator WYDEN.

Mr. WYDEN. Mr. President, I will be very brief. I know my colleague from New York, Senator SCHUMER, has a plane to catch.

Senator BURNS and I have worked for more than 4 years on this legislation, and it is particularly important that it pass today. Every single day, the flood of pornographic and sleazy spam grows. With this legislation, Congress is beginning to stem the tide. We understand that this is going to be a difficult battle because the kingpin spammers are not technological simpletons. No matter what law Congress passes, they are going to be very aggressive about trying to find evasive strategies to get around that. But I am of the view that with the passage of this legislation, if our prosecutors, the Federal Trade Commission, and the Attorney General come down on the kingpin spammers with hobnail boots, we can put in place a strategy that can stem this tide.

Suffice it to say, the spammers are going to go to great lengths to try to get around this law. We know, for example, that many of them are going to try to move offshore. It is going to be important to have international agreements that will also bring together U.S. authorities and international authorities against those who would try to get around this legislation.

It is important to remember what Congress is doing now; that is, Congress is saying spamming is an outlaw business. It is an outlaw business that is going to be treated as an area of priorities for prosecutors and law enforcement officials. That has not been the case in the past. Essentially, when Senator BURNS and I pursued this problem of spamming a number of years ago, a lot of people asked: Why in the world would a couple of U.S. Senators be tackling this issue? They intimated that it really wasn't worthy of the Senate's time. Spam has grown so extraordinarily in the last few years, and now people have been clammering about why the Senate isn't moving ahead with this legislation that they think is important because spam is such an intrusion into their lives every single day.

We have continued work to do. Senator SCHUMER will speak next. He has a very important idea with respect to trying to put in place a Do Not Spam list. It is a promising one. I think all of us would acknowledge there are some details to be worked out with the Federal Trade Commission. Senator CORZINE has done some very good work in looking at some creative ideas for the future. I intend to work closely with him because he has been a leader in the technology area. But I think we ought to understand that this effort today is the culmination of more than 4 years of hard work. It is not just needed, it is overdue.

We are not going to pretend this legislation is a silver bullet because we know that no piece of legislation is. But when this bill takes effect, the big-time spammers who up to this point faced no consequences, for all practical purposes, will suddenly be at risk for criminal prosecution, Federal Trade Commission enforcement, and million-dollar lawsuits by State attorneys general and Internet service providers.

I believe a number of these key enforcement actions will be taken immediately after this legislation is passed. This will set in place the kind of deterrent that is going to allow us to say it is a different day. The big-time spammers will face consequences when they flood our citizens and our families with the trash and the pornography. That is why this is an important step forward.

He is going to speak next, but I commend my colleague, the Senator from New York, for his usual persistence. He stayed at it by saying this was an important issue. We have wrestled with this question with respect to the Do Not Call list as well. I happen to think that the Senator from New York is certainly talking about a principle we need to address in the communications area. I happen to think the first amendment is special. People ought to have the right to communicate. But citizens also ought to have the right to say: We have had enough. We don't want to have people flooded with this kind of information. That is the principle that is at stake here. I commend the Senator from New York.

My partner, the chairman of the telecommunications subcommittee, is not in the Chamber. But I am proud to serve with him. He has been an exceptionally gracious ally on this for many years.

I am glad that this proconsumer measure, a measure that I think makes a beginning in efforts against big-time spammers, is passing. It will be of great benefit to consumers.

I yield the floor.

The PRESIDING OFFICER. The Senator from New York.

Mr. SCHUMER. Thank you, Mr. President.

First, let me thank my colleague from Oregon for his leadership on this issue, for his persistence—done in a slightly different way, the Oregon way, not the New York way, but it is effective, if not more effective—and for his understanding. There is no one in this Chamber who both understands technology issues and yet has a political grasp of politics and blends the two. I thank him for his leadership.

I thank the Senator from Montana, as well, who has worked long and hard on this issue; and my good friend from Arizona, the chairman of the Commerce Committee, also.

This is going to be a good Thanksgiving for consumers. We are dealing with spam today. The portability rules for cell phones have been enacted. I worked long and hard on those. Both antispamming legislation and portability rules are very important things we have done for consumers. As technology changes, we need to adapt the rules by which this technology can work. The basic principles we have always have to be applied in new and different ways. That is what we are trying to do today.

E-mail is one of the great inventions of the 20th century. But, unfortunately, if we did nothing, e-mail would not be around within a few years and no one could use it. What was an annoyance a few years ago has become a major problem this year and could really cripple e-mail a few years from now. So this Congress has acted. We acted in a thoughtful and careful way.

Is this bill going to solve everything? No. But will it make a real difference? You bet. Spammers: Be put on notice. Within a few months you will be committing a criminal act if you do what you are doing now.

With this bill, Congress is saying that if you are a spammer, you can wind up in the slammer. That is the bottom line. The bottom line is that there will be criminal penalties and real prosecution. Will we go after every spammer, somebody who makes a mistake here and there? No. But the studies show us—this is what gives all of us such hope—that maybe 250 spammers send out 90 percent of the e-mail. And we are saying to those 250, no matter where you are, or how you try to hide your spam, we will find you. This bill gives the FTC and the Justice Department the tools to go after you.

That is why this bill is so important. This is such a good day, not only for those who use computers but for technology in general.

I became familiar with this issue when I noticed my daughter on her computer. My wife and I had always said to one another: Isn't it great that instead of watching television, our kids are always on the computer? Then we saw what was popping up in their e-mail—things we wouldn't want to see, let alone my 14-year-old daughter. As we looked into it, we saw what was happening. Spam is annoying, crippling commerce, and pornographic. All of

that has to end while we preserve the essence of spam itself, which is ease of communication.

There is no single solution. That is why this bill is correct in taking the eclectic approach. I wanted to put a few more provisions in. I have talked to my friends from Montana and Oregon. We are going to monitor this. If new things are needed, we will add them. But there are many different ways we can go after spammers after this legislation is signed by the President.

The part for which I fought fiercely is the No Spam Registry. It will provide prosecutors with the best tools to create the case. They won't have to prove intent. They won't have to prove anything other than as they do with the No Call Registry. Day after day, spammers have relentlessly sent hundreds and thousands of spam e-mails to people who have explicitly said they do not want spam.

I believe that it will work. I know that the FTC has some doubts. Although, fortunately, they now say it is technically feasible, and they are not worried about the list being stolen, they are worried about the evidence.

My answer to the FTC: Try it. We do not have anything better. It is not going to solve everything, but it is the best tool we have.

When they come back to us in 6 months with their proposal, which they must do under this legislation, I have been assured by both Chairman MCCAIN and Ranking Member HOLLINGS, as well as Senators WYDEN and BURNS, that we will make sure they implement it. We will either do it statutorily or by pressure from the appropriators and others.

So the FTC may disagree with the vast majority of Americans and the unanimity of the Congress—I guess unanimous in the Senate, not quite in the House—but we are going to make this No Spam Registry a reality within a year.

So the bottom line is simple: For the first time there is some light at the end of the tunnel in the fight against spam. This legislation—not a panacea—will greatly reduce the burden of spam, the difficulty of spam, and the pornographic aspects of spam.

So again, I thank all of my colleagues in the Senate in letting this legislation go through. Again, it is a happy Thanksgiving to computer users everywhere.

I thank my colleagues from Montana and Oregon for their leadership. I thank Senators MCCAIN and HOLLINGS, as chairman and ranking member of the committee, for their support.

When the industry groups tried to rip the registry out of the legislation, these folks stood firm, the Senate stood firm, and that is why we have it in here today.

With that, Mr. President, let me just conclude by wishing you, my colleagues from Maine and Oregon, and all of my colleagues, and all those who work here, a very happy Thanksgiving.

For me, God has given me much to be thankful for, and I will dwell on that over the next few days. I hope everyone here feels the same way about their fortune and good fortune.

With that, I yield the floor.

ANTI-SPAN LEGISLATION

Mr. BURNS. Mr. President, I would like to engage the gentleman from Oregon, Mr. WYDEN, in a colloquy regarding some details of the anti-spam legislation approved by the Senate. We have worked tirelessly on S. 877, and it is important to ensure that spammers cannot get around the definitions of electronic mail address and electronic mail message that will be regulated under this law. The definitions in the bill require electronic mail addresses to contain a domain part. This requirement is important to make sure we only capture e-mail and do not regulate other communications platforms, such as Instant Messaging. However, I want to be clear that the intent of Congress is to capture e-mail messages as that term is commonly understood. This includes e-mail messages sent within the same domain that may not actually display the domain part of the e-mail address.

Mr. WYDEN. I thank the gentleman from Montana for raising this important issue. Yes, the intent of S. 877 is to capture all e-mail messages as that term is commonly understood. This includes e-mail messages where the domain part of the address may not be displayed. That is why the bill's definition of e-mail address, in referring to the domain part, contains the phrase ''whether or not displayed.'' We certainly do not want to create any loopholes that spammers could potentially exploit and I appreciate the opportunity to clarify this point.

Mr. BURNS. I would like to flag one other aspect of the bill. Under section 6, the FTC can bring enforcement actions against merchants whose products are promoted in spam e-mails, even if the merchant is not the spammer. Isn't that correct?

Mr. WYDEN. I agree with the Senator.

Mr. BURNS. But isn't it also true that section 5 can be used against merchants whose products are promoted in spam e-mails? Can't the FTC, State A.G.s, and Internet Service Providers bring actions under section 5 against parties who aren't themselves spamming, but rather hire spammers to promote their products or services?

Mr. WYDEN. Absolutely. The bill's definition of ''initiate'' makes that clear, because it applies not only to the spammer that originates the actual e-mail, but also to a party who has hired or otherwise induced the spammer to send the e-mail on its behalf. If the e-mail message violates the bill, both parties would be on the hook under section 5, and enforcement would be possible against both or either parties.

Mr. BURNS. That confirms my understanding. So what is different about section 6, as I understand it, is that section 6 does not require any showing that the merchant actually hired or induced the spammer to send the spam. In other words, if the spammer is hard to find and his contractual relationship with the merchant has been obscured by under-the-table dealings, the FTC doesn't have to spend time and effort trying to prove the relationship.

Mr. WYDEN. I share the Senator's understanding of how section 6 differs from the provisions of section 5. I would only add that the drafters considered which parties should have the discretion to enforce the bill in the manner set forth in section 6, and decided that section 6 should be enforced by the FTC only.

Mr. BURNS. I thank my colleague from Oregon.

Mr. LEAHY. Mr. President, I am pleased that the Senate is passing legislation to help staunch the torrent of unwanted commercial e-mail, commonly known as spam. During the past year, I worked closely with Senator HATCH and other members of the Judiciary Committee to craft criminal penalties for a variety of spammer tactics. Those penalties, which we introduced in June as part of the Criminal Spam Act, S. 1293, are included in the broader anti-spam legislation that we pass today. The bill will now go back to the House of Representatives for final approval, and then to the President for signing.

Spam is much more than a technological nuisance. In the past few years, it has become a serious and growing problem that threatens to undermine the vast potential of the Internet.

Businesses and individuals currently wade through tremendous amounts of spam in order to access e-mail that is of relevance to them—and this is after Internet Service Providers, businesses, and individuals have spent time and in some cases enormous amounts of money blocking a large percentage of spam from reaching its intended recipients.

In my home State of Vermont, one legislator recently found that two-thirds of the 96 e-mails in his inbox were spam. And this occurred after the legislature had installed new spam-blocking software on its computer system that seemed to be catching 80 percent of the spam. The assistant attorney general in Vermont was forced to suggest to computer users the following means to avoid these unsolicited commercial e-mails: ''It's very bad to reply, even to say don't send anymore. It tells the spammer they have a live address . . . The best thing you can do is just keep deleting them. If it gets really bad, you may have to change your address.'' This experience is echoed nationwide.

E-mail users are having the online equivalent of the experience of the woman in the Monty Python skit, who seeks to order a Spam-free breakfast at a restaurant. Try as she might, she cannot get the waitress to bring her the meal she desires. Every dish in the

restaurant comes with Spam; it is just a matter of how much. There is ''egg, bacon and Spam''; ''egg, bacon, sausage and Spam''; ''Spam, bacon, sausage and Spam''; ''Spam, egg, Spam, Spam, bacon and Spam''; ''Spam, sausage, Spam, Spam, bacon, Spam, tomato and Spam''; and so on. Exasperated, the woman finally cries out: ''I don't like Spam! . . . I don't want ANY Spam!''

Individuals and businesses are understandably reacting similarly to electronic spam. A Harris poll taken late last year found that 80 percent of respondents view spam as ''very annoying,'' and fully 74 percent of respondents favor making mass spamming illegal. Earlier this month, more than three out of four people surveyed by Yahoo! Mail said it was ''less aggravating to clean a toilet'' than to sort through spam. Americans are fed up.

Some 30 States now have anti-spam laws, but the globe-hopping nature of e-mail makes these laws difficult to enforce. Technology will undoubtedly play a key role in fighting spam, but a technological solution to the problem is not likely in the foreseeable future. ISPs block billions of unwanted e-mails each day, but spammers are winning the battle.

Millions of unwanted, unsolicited commercial e-mails are received by American businesses and individuals each day, despite their own, additional filtering efforts. Ferris Research has estimated that spam costs U.S. firms $8.9 billion annually in lost worker productivity, consumption of bandwidth, and the use of technical support to configure and run spam filters and provide helpdesk support for spam recipients.

The costs of spam are significant to individuals as well, including time spent identifying and deleting spam, inadvertently opening spam, installing and maintaining anti-spam filters, tracking down legitimate messages mistakenly deleted by spam filters, and paying for the ISP's blocking efforts.

And there are other prominent and equally important costs of spam. It may introduce viruses, worms, and ''Trojan horse'' programs—that is, programs that unsuspecting users download onto their computers that are designed to take control of those computers—into personal and business computer systems, including those that support our national infrastructure.

Spammers are constantly in need of new machines through which to route their garbage e-mail, and a virus makes a perfect delivery mechanism for the engine they use for their mass mailings. Some analysts said the SoBigF virus may have been created with a more malicious intent than most viruses, and may even be linked to spam e-mail schemes that could be a source of cash for those involved in the scheme.

The interconnection between computer viruses and spam is readily apparent: Both flood the Internet in an attempt to force a message on people who would not otherwise choose to receive it. Criminal laws I wrote prohibiting the former have been invoked and enforced from the time they were passed. It is the latter dilemma we must now confront.

Spam is also fertile ground for deceptive trade practices. The FTC has estimated that 90 percent of the spam involving investment and business opportunities, and nearly half of the spam advertising health products and services, and travel and leisure, contains false or misleading information.

This rampant deception has the potential to undermine Americans' trust of valid information on the Internet. Indeed, it has already caused some Americans to refrain from using the Internet to the extent they otherwise would. For example, some have chosen not to participate in public discussion forums, and are hesitant to provide their addresses in legitimate business transactions, for fear that their e-mail addresses will be harvested for junk e-mail lists. And they are right to be concerned. The FTC found spam arriving at its computer system just 9 minutes after posting an e-mail address in an online chat room.

I have often said that Congress must exercise great caution when regulating in cyberspace. Any legislative solution to spam must tread carefully to ensure that we do not impede or stifle the free flow of information on the Internet. The United States is the birthplace of the Internet, and the whole world watches whenever we decide to regulate it. Whenever we choose to intervene in the Internet with Government action, we must act carefully, prudently, and knowledgeably, keeping in mind the implications of what we do and how we do it. And we must not forget that spam, like more traditional forms of commercial speech, is protected by the first amendment.

At the same time, we must not allow spam to result in the ''virtual death'' of the Internet, as one Vermont newspaper put it.

The Internet is a valuable asset to our Nation, to our economy, and to the lives of Americans, and we should act prudently to secure its continued viability and vitality.

On June 19 of this year, Senator HATCH and I introduced S. 1293, the Criminal Spam Act, together with several of our colleagues on the Judiciary Committee. On September 25, the Committee unanimously voted to report S. 1293 to the floor. On October 22, the Senate unanimously adopted the criminal provisions of the bill as an amendment to S. 877, the CAN SPAM Act. Today, the Senate is passing these same criminal provisions as section 4 of a modified version of S. 877, as passed by the House last week.

The Hatch-Leahy criminal provisions prohibit five principal techniques that spammers use to evade filtering software and hide their trails.

First, our legislation prohibits hacking into another person's computer system and sending bulk spam from or through that system. This criminalizes the common spammer technique of obtaining access to other people's e-mail accounts on an ISP's e-mail network, whether by password theft or by inserting a Trojan horse to send bulk spam.

Second, our legislation prohibits using a computer system that the owner makes available for other purposes as a conduit for bulk spam, with the intent of deceiving recipients as to the spam's origins. This prohibition criminalizes another common spammer technique—the abuse of third parties' ''open'' servers, such as e-mail servers that have the capability to relay mail, or Web proxy servers that have the ability to generate ''form'' mail.

Spammers commandeer these servers to send bulk commercial e-mail without the server owner's knowledge, either by ''relaying'' their e-mail through an ''open'' e-mail server, or by abusing an ''open'' Web proxy server's capability to generate form e-mails as a means to originate spam, thereby exceeding the owner's authorization for use of that e-mail or Web server. In some instances the hijacked servers are even completely shut down as a result of tens of thousands of undeliverable messages generated from the spammer's e-mail list.

The legislation's third prohibition targets another way that outlaw spammers evade ISP filters: Falsifying the ''header information'' that accompanies every e-mail, and sending bulk spam containing that fake header information. More specifically, the legislation prohibits forging information regarding the origin of the e-mail message, and the route through which the message attempted to penetrate the ISP filters.

At the suggestion of the Department of Justice, this third offense has been amended since the Senate last considered it to require a showing of materiality. This means the Government must prove that the header information was 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 title, or a law enforcement agency, to identify, locate, or respond to the person who initiated the e-mail or to investigate the alleged violation.

Fourth, the Hatch-Leahy legislation prohibits registering for multiple e-mail accounts or Internet domain names using false identities, and sending bulk e-mail from those accounts or domains. This provision targets deceptive ''account churning,'' a common outlaw spammer technique that works as follows. The spammer registers—usually by means of an automatic computer program—for large numbers of e-mail accounts or domain names, using false registration information, then sends bulk spam from one account or

domain after another. This technique stays ahead of ISP filters by hiding the source, size, and scope of the sender's mailings, and prevents the e-mail account provider or domain name registrar from identifying the registrant as a spammer and denying his registration request. Falsifying registration information for domain names also violates a basic contractual requirement for domain name registration falsification. As with the last offense, this offense now requires that the registration information be falsified ''materially.''

Fifth and finally, our legislation addresses a major hacker spammer technique for hiding identity that is a common and pernicious alternative to domain name registration—hijacking unused expanses of Internet address space and using them as launch pads for junk e-mail. Hijacking Internet Protocol—IP—addresses is not difficult: Spammers simply falsely assert that they have the right to use a block of IP addresses, and obtain an Internet connection for those addresses. Hiding behind those addresses, they can then send vast amounts of spam that is extremely difficult to trace.

Penalties for violations of these new criminal prohibitions are tough but measured. Recidivists and those who send spam in furtherance of another felony may be imprisoned for up to 5 years. Large-volume spammers, those who hack into another person's computer system to send bulk spam, and spam ''kingpins'' who use others to operate their spamming operations may be imprisoned for up to 3 years. Other offenders may be fined and imprisoned for no more than one year. Convicted offenders are also subject to forfeiture of proceeds and instrumentalities of the offense.

In addition to these penalties, the Hatch-Leahy legislation directs the Sentencing Commission to consider providing sentencing enhancements for those convicted of the new criminal provisions who obtained e-mail addresses through improper means, such as harvesting, and those who knowingly sent spam containing or advertising a falsely registered Internet domain name. We have also worked with Senator NELSON on language directing the Sentencing Commission to consider enhancements for those who commit other crimes that are facilitated by the sending of spam.

I should note that the Criminal Spam Act, from which these provisions are taken, enjoys broad support from ISPs, direct marketers, consumer groups, and civil liberties groups alike. Again, the purpose of these criminal provisions is to deter the most pernicious and unscrupulous types of spammers—those who use trickery and deception to induce others to relay and view their messages. Ridding America's inboxes of deceptively delivered spam will help clear electronic channels for Internet users from coast-to-coast. But it is not a cure-all for the spam pandemic.

The fundamental problem inherent to spam—its sheer volume—may well persist even in the absence of fraudulent routing information and false identities. In a recent survey, 82 percent of respondents considered unsolicited bulk e-mail, even from legitimate businesses, to be unwelcome spam. Given this public opinion, and in light of the fact that spam is, in essence, cost-shifted advertising, we need to take a more comprehensive approach to our fight against spam.

While I am generally supportive of the CAN SPAM Act, it does raise some concerns. For one thing, it may not be tough enough to do the job.

The bill takes an ''opt out'' approach to spam—that is, it requires all commercial e-mail to include an ''opt out'' mechanism, by which e-mail recipients may opt out of receiving further unwanted spam. My concern is that this approach authorizes spammers to send at least one piece of spam to each e-mail address in their database, while placing the burden on e-mail recipients to respond. People who receive dozens, even hundreds, of unwanted e-mails each day may have little time or energy for anything other than opting-out from unwanted spam. Meantime, CAN SPAM will sweep away dozens of State anti-spam laws, including some that were substantially more restrictive.

I am also troubled by the two labeling requirement in the CAN SPAM Act. The first makes it unlawful to send an unsolicited commercial e-mail message unless it provides, among other things, ''clear and conspicuous identification that the message is an advertisement or solicitation,'' and ''a valid physical postal address of the sender.'' The second—added as a floor amendment during Senate consideration of the bill in October—requires ''warning labels'' on any commercial e-mail that includes ''sexually oriented material.''

While we all want to curb spam and protect our children from inappropriate material, there are important first amendment concerns to regulating commercial e-mail in ways that require specific labels on protected speech. Such requirements inhibit both the speaker's right to express and the listener's right to access constitutionally protected material.

In addition, the bill's definition of ''sexually oriented material'' as any material that ''depicts'' sexually explicit conduct seems overly broad. According to Webster's dictionary, ''depict'' may mean either to represent by a picture or to describe in words. It is my hope that the FTC, which has some rulemaking authority with respect to this labeling requirement, will clarify that it applies to ''visual'' depictions only.

The CAN SPAM Act may not be perfect, but it is a serious effort to address a difficult and urgent problem. I support its passage today, and commend the bipartisanship that was needed to get this done.

Mr. BURNS. Mr. President, I rise today to support the final passage of the CAN–SPAM bill, which will help to stem the tide of junk e-mail that is flooding the Nation's inboxes. I want to specifically thank my colleague Senator WYDEN, the coauthor of the bill, who has been working tirelessly on this issue for years. Thanks to discussions over the past few days, many of the already-strong proconsumer provisions in CAN–SPAM have been enhanced. The bill the Senate considers today contains substantial statutory damages for spammers and additional notice requirements on commercial e-mail.

The extent of bipartisan cooperation on this issue is no surprise given the deluge of spam consumers face in their inboxes everyday. The costs to businesses and individuals are escalating and wide ranging. Businesses lose money when employees take more and more time to wade through their e-mails. Servers all over the country have difficulty blocking spam, all while spammers work to find more and more ways to circumvent the latest software, server, or individual blocking systems.

Spam is particularly harmful to rural areas. Because of the vast distances in Montana, many of my constituents are forced to pay long distance charges for their time on the Internet. Spam makes it nearly impossible for those in rural America to realize the tremendous economic and educational benefits of the online era.

The CAN–SPAM bill empowers consumers and grants additional enforcement authority to the Federal Trade Commission to take action against spammers. The bill requires the senders of commercial e-mail to include a clear ''opt-out'' mechanism to allow consumers to be removed from mass e-mail lists. This ''opt-out'' must also be clearly described in the e-mail itself, so that users of e-mail are not forced to sift through pages of legalese to determine where they can stop unwanted e-mail.

The senders of commercial e-mail must also provide a valid physical postal address so that they are not able to hide their identities. Finally, e-mail marketers must include notice that the e-mail is an advertisement. Simply put, the CAN–SPAM bill finally gives consumers a measure of control over their inboxes.

In cases where e-mail marketers don't comply with the CAN–SPAM bill, the penalties are severe. Spammers are on the hook for damages up to $250 per spam e-mail with a cap of $2 million. This already high penalty can be tripled if particularly unethical methods are used, such as ''computer hijacking'' to send spam by taking control of the computers of legitimate users without their knowledge or for harvesting addresses from legitimate Web sites to send spam. For criminal spammers who try to hide their identities by using false header information, damages are not capped.

The CAN–SPAM bill also includes enhanced enforcement authority for the FTC to close possible loopholes for spammers and to keep up with technological developments. Granting the Commission the ability to keep pace with the new techniques of spammers is essential because it has become clear in recent years that these criminals are growing increasingly sophisticated in their methods.

The passage of CAN–SPAM today will help to stem the tide of the toxic sea of spam. Clearly, consumers have been demanding control over their e-mail inboxes and the passage of CAN–SPAM today will give consumers a key victory in the battle against criminal spammers.

The PRESIDING OFFICER (Mr. CORNYN). The Senator from Maine.

Ms. COLLINS. Mr. President, let me first return the Thanksgiving greetings of my colleagues. I hope that they, too, are able to have a happy holiday with their families and friends.

INVESTIGATION INTO THE LACK OF COORDINATION BETWEEN FEDERAL AGENCIES

Ms. COLLINS. Mr. President, last week NBC News aired a report indicating that suspected terrorists had been granted American citizenship or permanent residency at the same time they were under investigation by the FBI for their involvement in terrorism. This well-researched piece reached the warranted and troubling conclusion that this occurred despite advance knowledge within the Department of Justice.

The NBC report revealed an alarming and dangerous lack of coordination between Federal agencies. The NBC piece parallels credible allegations that first came to my attention in January.

As the chairman of the Committee on Governmental Affairs, to followup on these allegations, I have made repeated requests of the Department of Justice for information that would allow my committee to assess this potentially serious threat to our national security.

We have a saying up in Maine: You can't get there from here. You may have heard it, Mr. President. But when it comes to travel in my home State, it is not really true. The roads may be winding, and the route may not be all that direct, but with persistence and patience, you can always get where you need to go.

However, when it comes to dealing with the Department of Justice on this very serious matter, it seems that you cannot get anywhere. I have been persistent, but my patience has pretty much run out.

The allegations that I received in January were these: In the course of investigating foreign-born individuals for terrorism-related offenses, the FBI learned that some of these individuals were in the process of applying for naturalization or permanent residency.

FBI agents requested permission to share that critical important information with the INS. Their FBI supervisors, however, refused those requests. This information has been confirmed by NBC News's chief investigative reporter, Lisa Myers, in her thoroughly researched piece that aired last week.

My requests to the Department of Justice for information that would define the size of this alleged hole in national security and of this possible gap in interagency cooperation have been refused repeatedly.

I have modified my requests in order to accommodate the specific objections raised by the Department. My modified requests have also been refused due to new objections or, in some cases, old ones simply rephrased.

Here is a brief travelogue of my 10-month journey in the bureaucracy of the Department of Justice: On January 21, shortly after these allegations came to my attention, I wrote to the FBI Director, Robert Mueller, and asked that he provide the committee with the names, dates of birth, INS registration numbers, and start dates of investigations of all persons who have been the subjects of terrorism investigations from September 10, 1991, through September 10, 2001, in the 15 largest FBI field offices. I asked to have this information delivered to my office by February 4.

Well, I received no response at all until February 28, when I received a reply from the Department categorically denying my request. The primary reason cited was that the Department had a longstanding policy of not providing Congress with information about people who have been investigated but not prosecuted.

Among the other supporting reasons were the separation of powers and—I am not making this up, Mr. President—a concern that providing Congress with information that could help it understand and remedy a situation so potentially damaging to our Nation's security could, and I quote, ''gravely damage the nation's security.''

The Department did offer, at that point, to work with me to see if there was an alternative. I eagerly took the Department up on that offer, and I wanted to try to accommodate whatever legitimate concerns the Department might have.

Thus, my staff talked repeatedly with the Department during the next few months to craft a mutually agreeable alternative approach.

On May 21, I submitted another much narrower request proposing that the Department of Justice would conduct its own review, a review I would think that the Department would be very eager to conduct once this threat was brought to the Department's own attention. Moreover, the length of the review would be reduced from a decade to 5 years, and the scope would be reduced from 15 field offices to just 5.

Now, by this time, of course, the INS had been moved from the Department of Justice to the new Department of Homeland Security.

It had been renamed as the Bureau of Citizenship and Immigration Services. I suggested the FBI provide the results of its internal review to the BCIS so it could determine who had been granted citizenship or permanent residency while they were being investigated for terrorism. Again, I would think the Department would be very concerned about the serious breakdown and lapse in communication and would be eager to review its own files to quickly uncover the names of individuals who might have become citizens or permanent residents while they were under investigation for terrorism-related activities.

After months of negotiations between my staff and the Department's staff, I believed I had finally come up with a solution that addressed all of the Department's concerns.

On July 3—keep in mind how much more time has yet elapsed—I received a reply. Much to my astonishment, the answer once again was no.

Two new concerns were raised: First, when the FBI and the INS were part of the same overall Department of Justice, they could share information for this purpose legally; although, as we well know, they didn't. Now that they are in two different departments, the Justice Department claims the Privacy Act prevents the sharing of this critical information.

The second reason advanced was the FBI simply did not have the time or resources to review its own files. Again, keep in mind how important it is for the Department to know how many people were in this situation where they were under investigation for terrorism and yet received either American citizenship or permanent residency. I would think the FBI, on its own volition, would be eager to retrieve that information.

At this point some of my Senate colleagues may be asking themselves a few questions, if they have had some experience with congressional oversight. First, hasn't the Justice Department many times in the past provided Congress with information such as interview summaries and documentary evidence related to individuals who have been investigated but not prosecuted? Second, does this refute the Justice Department's argument about a supposedly sacrosanct longstanding policy? Would such a policy, if it existed and were adhered to as strictly as the Justice Department now asserts, exempt the Justice Department from effective congressional oversight? The answer to these questions is obvious.

Although the Justice Department would not review its own files to discover the extent of this problem and to document whether terrorists had been granted citizenship or permanent residency, its officials have indicated in writing to me that this likely occurred.

Let me expand on that point. The Justice Department is not refuting the basic premise. In a July 3 letter I received from the Department, from which I want to quote, it says: