AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

107TH CONGRESS, 1st Session | HOUSE OF REPRESENTATIVES | REPT. 107–41 Part 1

UNSOLICITED COMMERCIAL ELECTRONIC MAIL ACT OF 2001

APRIL 4, 2001.—Ordered to be printed

Mr. TAUZIN, from the Committee on Energy and Commerce, submitted the following

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 718]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 718) to protect individuals, families, and Internet service providers from unsolicited and unwanted electronic mail, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

	Page
Amendment	1
Purpose and Summary	8
Background and Need for Legislation	8
Hearings	10
Committee Consideration	10
Committee Votes	10
Committee Oversight Findings	11
Performance Goals and Objectives	11
New Budget Authority, Entitlement Authority, and Tax Expenditures	11
Committee Cost Estimate	11
Congressional Budget Office Estimate	11
Federal Mandates Statement	11
Advisory Committee Statement	12
Constitutional Authority Statement	12
Applicability to Legislative Branch	12
Section-by-Section Analysis of the Legislation	12
Changes in Existing Law Made by the Bill, as Reported	17

AMENDMENT

The amendment is as follows:

89–006

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Unsolicited Commercial Electronic Mail Act of 2001".

SEC. 2. CONGRESSIONAL FINDINGS AND POLICY.

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

(1) There is a right of free speech on the Internet.

(2) The Internet has increasingly become a critical mode of global communication and now presents unprecedented opportunities for the development and growth of global commerce and an integrated worldwide economy. In order for global commerce on the Internet to reach its full potential, individuals and entities using the Internet and other online services should be prevented from engaging in activities that prevent other users and Internet service providers from having a reasonably predictable, efficient, and economical online experience.

(3) Unsolicited commercial electronic mail can be an important mechanism through which businesses advertise and attract customers in the online environment.

(4) 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.

(5) Unsolicited commercial electronic mail may impose significant monetary costs on 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. The sending of such mail is increasingly and negatively affecting the quality of service provided to customers of Internet access service, and shifting costs from the sender of the advertisement to the Internet access service.

(6) While some senders of unsolicited commercial electronic mail messages provide simple and reliable ways for recipients to reject (or "opt-out" of) receipt of unsolicited 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.

(7) An increasing number of senders of unsolicited commercial electronic mail purposefully disguise the source of such mail so as to prevent recipients from responding to such mail quickly and easily.

(8) Many senders of unsolicited commercial electronic mail collect or harvest electronic mail addresses of potential recipients without the knowledge of those recipients and in violation of the rules or terms of service of the database from which such addresses are collected.

(9) Because recipients of unsolicited commercial electronic mail are unable to avoid the receipt of such mail through reasonable means, such mail may invade the privacy of recipients.

(10) In legislating against certain abuses on the Internet, Congress should be very careful to avoid infringing in any way upon constitutionally protected rights, including the rights of assembly, free speech, and privacy.

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

(1) there is substantial government interest in regulation of unsolicited commercial electronic mail;

(2) Internet service providers should not be compelled to bear the costs of unsolicited commercial electronic mail without compensation from the sender; and

(3) recipients of unsolicited commercial electronic mail have a right to decline to receive or have their children receive unsolicited commercial electronic mail.

SEC. 3. DEFINITIONS.

In this Act:

(1) AFFILIATE.—The term "affiliate" means, with respect to an entity, any other entity that—

(A) controls, is controlled by, or is under common control with such entity; and

(B) provides marketing information to, receives marketing information from, or shares marking information with such entity.

(2) CHILDREN.—The term "children" includes natural children, stepchildren, adopted children, and children who are wards of or in custody of the parent,

who have not attained the age of 18 and who reside with the parent or are under his or her care, custody, or supervision.

(3) COMMERCIAL ELECTRONIC MAIL MESSAGE.—The term "commercial electronic mail message" means any electronic mail message that primarily advertises or promotes the commercial availability of a product or service for profit or invites the recipient to view content on an Internet web site that is operated for a commercial purpose. An electronic mail message shall not be considered to be a commercial electronic mail message solely because such message includes a reference to a commercial entity that serves to identify the initiator.

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

(5) 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.

(6) ELECTRONIC MAIL ADDRESS.—

(A) IN GENERAL.—The term "electronic mail address" means a destination (commonly expressed as a string of characters) to which electronic mail can be sent or delivered.

(B) INCLUSION.—In the case of the Internet, the term "electronic mail address" may include an electronic mail address consisting of a 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").

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

(8) INITIATE.—The term "initiate", when used with respect to a commercial electronic mail message, means to originate such message or to procure the origination of such message.

(9) INITIATOR.—The term "initiator", when used with respect to a commercial electronic mail message, means the person who initiates such message. Such term does not include a provider of an Internet access service, or any other person, whose role with respect to the message is limited to the transmission, routing, relaying, handling, or storing, through an automatic technical process, of a message originated by others.

(10) INTERNET.—The term "Internet" has the meaning given that term in section 231(e)(3) of the Communications Act of 1934 (47 U.S.C. 231(e)(3)).

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

(A) the message falls within the scope of an express and unambiguous invitation or consent granted by the recipient and not subsequently revoked;

(B) the recipient had clear and conspicuous notice, at the time such invitation or consent was granted, of—

(i) the fact that the recipient was granting the invitation or consent;

(ii) the scope of the invitation or consent, including what types of commercial electronic mail messages would be covered by the invitation or consent and what senders or types of senders, if any, other than the party to whom the invitation or consent was communicated would be covered by the invitation or consent; and

(iii) a reasonable and effective mechanism for revoking the invitation or consent; and

(C) the recipient has not, after granting the invitation or consent, submitted a request under section 5(a)(1) not to receive unsolicited commercial electronic mail messages from the initiator.

(13) PRE-EXISTING BUSINESS RELATIONSHIP.—The term "pre-existing business relationship" means, when used with respect to the initiator and recipient of a commercial electronic mail message, that—

(A) within the 5-year period ending upon receipt of such message, there has been a business transaction (including a transaction involving the provision, free of charge, of information, goods, or services, that were requested by the recipient) between—

(i) the initiator or any affiliate of the initiator; and

(ii) the recipient; and

(B) the recipient was, at the time of such transaction or thereafter or in the transmission of the commercial electronic mail message, provided a clear and conspicuous notice of an opportunity not to receive further mes-

sages from the initiator and any affiliates of the initiator and has not exercised such opportunity.

(14) RECIPIENT.—The term "recipient", when used with respect to a commercial electronic mail message, means the addressee of such message. If an addressee of a commercial electronic mail message has one or more electronic mail addresses in addition to the address to which the message was addressed, the addressee shall be treated as a separate recipient with respect to each such address.

(15) UNSOLICITED COMMERCIAL ELECTRONIC MAIL MESSAGE.—The term "unsolicited commercial electronic mail message" means any commercial electronic mail message that is sent to a recipient—

(A) without prior recipient consent; and

(B)(i) with whom the initiator does not have a pre-existing business relationship;

(ii) by an initiator or any affiliate of the initiator after the recipient requests, pursuant to section 5(a)(1), not to receive further commercial electronic mail messages from that initiator; or

(iii) by a person or any affiliate of the person after the expiration of a reasonable period of time after the recipient requests, pursuant to section 5(a)(2), to be removed from the distribution lists under the control of a person.

SEC. 4. CRIMINAL PENALTY FOR UNSOLICITED COMMERCIAL ELECTRONIC MAIL CONTAINING FRAUDULENT ROUTING INFORMATION.

Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a)(5)—

(A) in subparagraph (B), by striking "or" at the end;

(B) in subparagraph (C), by inserting "or" after the semicolon at the end; and

(C) by adding at the end the following new subparagraph:

"(D) intentionally initiates the transmission of any unsolicited commercial electronic mail message to a protected computer in the United States with knowledge that any domain name, header information, date or time stamp, originating electronic mail address, or other information identifying the initiator or the routing of such message, that is contained in or accompanies such message, is false or inaccurate;";

(2) in subsection (c)(2)(A)—

(A) by inserting "(i)" after "in the case of"; and

(B) by inserting before "; and" the following: ", or (ii) an offense under subsection (a)(5)(D) of this section"; and

(3) in subsection (e)—

(A) by striking "and" at the end of paragraph (8);

(B) by striking the period at the end of paragraph (9) and inserting "; and"; and

(C) by adding at the end the following new paragraph:

"(10) the terms 'initiate', 'initiator', 'unsolicited commercial electronic mail message', and 'domain name' have the meanings given such terms in section 3 of the Unsolicited Commercial Electronic Mail Act of 2001.".

SEC. 5. OTHER PROTECTIONS AGAINST UNSOLICITED COMMERCIAL ELECTRONIC MAIL.

(a) REQUIREMENTS FOR TRANSMISSION OF MESSAGES.—

(1) INCLUSION OF RETURN ADDRESS IN COMMERCIAL ELECTRONIC MAIL.—It shall be unlawful for any person or affiliate of such person to initiate the transmission of a commercial electronic mail message to any person within the United States unless such message contains a valid electronic mail address, conspicuously displayed, to which a recipient may send a reply to the initiator to indicate a desire not to receive any further messages from the initiator and any affiliates of the initiator.

(2) PROHIBITION OF TRANSMISSION OF UNSOLICITED COMMERCIAL ELECTRONIC MAIL AFTER OBJECTION.—If a recipient makes a request to a person to be removed from all distribution lists under the control of such person, after receipt of such request—

(A) it shall be unlawful for such person or any affiliate of such person to initiate the transmission of an unsolicited commercial electronic mail message to such a recipient within the United States after the expiration of a reasonable period of time for removal from such lists;

(B) such person and affiliates (and the agents or assigns of the person or affiliate) shall delete or suppress the electronic mail addresses of the recipient from all mailing lists owned or controlled by such person or affiliate

(or such agents or assigns) within a reasonable period of time for such deletion or suppression; and

(C) it shall be unlawful for such person or affiliate (or such agents or assigns) to sell, lease, exchange, license, or engage in any other transaction involving mailing lists bearing the electronic mail addresses of the recipient.

(3) INCLUSION OF IDENTIFIER, OPT-OUT, AND PHYSICAL ADDRESS IN UNSOLICITED COMMERCIAL ELECTRONIC MAIL.—It shall be unlawful for any person to initiate the transmission of any unsolicited commercial electronic mail message to any person within the United States unless the message provides, in a manner that is clear and conspicuous to the recipient—

(A) identification that the message is an unsolicited commercial electronic mail message;

(B) notice of the opportunity under paragraph (2) to decline to receive further unsolicited commercial electronic mail messages from the initiator or any affiliate of the initiator; and

(C) the physical mailing address of the initiator.

(4) TREATMENT OF INTERNAL OPT-OUT LISTS.—If the policy of a provider of Internet access service requires compensation specifically for the transmission of unsolicited commercial electronic mail messages into its system, it shall be unlawful for the provider to fail to provide an option to its subscribers not to receive any unsolicited commercial electronic mail messages, except that such option shall not be required for any subscriber who has agreed to receive unsolicited commercial electronic mail messages in exchange for discounted or free Internet access service.

(5) AFFIRMATIVE DEFENSE.—It shall be an affirmative defense in any action or proceeding brought for a violation of any paragraph of this subsection that the violation was not intentional.

(b) CONDITIONS FOR ENFORCEMENT BY PROVIDERS OF INTERNET ACCESS SERVICE.—

(1) AUTHORITY TO OPT OUT.—After the expiration of a reasonable period of time for taking any action necessary to comply with a request under subparagraph (B) that begins upon the receipt of such a request, it shall be unlawful for a person or any affiliate of such person to initiate the transmission of an unsolicited commercial electronic mail message, to any recipient within the United States, that uses the equipment of a provider of Internet access service to recipients of electronic mail messages for such transmission, if such provider—

(A)(i) has in effect a policy that meets the requirements under paragraph (2); or

(ii) has received a significant number of complaints from its bona fide subscribers that they have received unsolicited commercial electronic mail messages from such person; and

(B) makes a request to such person by means of an electronic mail message not to use the equipment of the provider for the transmission of any unsolicited commercial electronic mail message.

(2) UCE POLICY.—A policy of a provider of Internet access service to recipients meets the requirements under this paragraph only if—

(A) it is a policy regarding the use of the equipment of the provider for the transmission of unsolicited commercial electronic mail messages that prohibits the transmission, using such equipment, of all such messages;

(B) the provider of Internet access service is making a good faith effort to block the transmission of all unsolicited commercial electronic mail messages that use the equipment of provider for such transmission;

(C) the policy is made publicly available by clear and conspicuous posting on a World Wide Web site of the provider of Internet access service, which has an Internet domain name that is identical to the Internet domain name of the electronic mail address to which the prohibition referred to in subparagraph (A) applies; and

(D) the provider of Internet access service informs each subscriber to such service of the policy.

(c) RULE OF CONSTRUCTION.—Nothing in this Act shall be construed—

(1) to prevent or limit, in any way, a provider of Internet access service from adopting a policy regarding commercial or other electronic mail, including a policy of declining to transmit certain types of electronic mail messages, and from enforcing such policy through technical means, through contract, or pursuant to any remedy available under any other provision of Federal, State, or local criminal or civil law; or

(2) to render lawful any such policy that is unlawful under any other provision of law.

(d) PROTECTION OF INTERNET ACCESS SERVICE PROVIDERS GOOD FAITH EFFORTS TO BLOCK TRANSMISSIONS.—A provider of Internet access service shall not be liable, under any Federal, State, or local civil or criminal law, for any action it takes in good faith to block the transmission or receipt of unsolicited commercial electronic mail messages.

SEC. 6. ENFORCEMENT.

(a) ENFORCEMENT THROUGH FTC ACT.—

(1) ENFORCEMENT.—Except as otherwise provided in this Act, section 5 shall be enforced by the Commission under the FTC Act.

(2) UNFAIR OR DECEPTIVE PRACTICE.—Any violation of section 5 shall be treated as a violation of a rule under section 18 of the FTC Act (15 U.S.C. 57a) regarding unfair or deceptive acts or practices.

(3) SCOPE OF COMMISSION ENFORCEMENT.—The Commission shall prevent any person from violating section 5 of 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 FTC Act were incorporated into and made a part of this section. Any person who violates section 5 of this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the FTC 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 FTC Act were incorporated into and made a part of this section.

(4) PROHIBITION OF REGULATIONS.—Neither the Commission nor any other Federal department or agency shall have any authority to issue any regulations to implement the provisions of this Act.

(b) PRIVATE RIGHT OF ACTION.—

(1) ACTIONS AUTHORIZED.—A recipient or a provider of Internet access service may, if otherwise permitted by the laws or rules of court of a State, bring in an appropriate court of that State, or may bring in an appropriate Federal court if such laws or rules do not so permit, either or both of the following actions:

(A) An action based on a violation of section 5 to enjoin such violation.

(B) An action to recover for actual monetary loss from such a violation in an amount equal to the greater of—

(i) the amount of such actual monetary loss; or

(ii) $500 for each such violation, not to exceed a total of $50,000.

(2) ADDITIONAL REMEDIES.—If the court finds that the defendant willfully or repeatedly violated section 5, the court may, in its discretion, increase the amount of the award to an amount equal to not more than three times the amount available under paragraph (1).

(3) ATTORNEY FEES.—In any such action, 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.

(4) PROHIBITION OF CLASS ACTIONS.—A private action arising under this subsection may not be brought as a plaintiff class action pursuant to the Federal Rules of Civil Procedure nor as a plaintiff class action pursuant to the law or rules of procedure of any State.

(5) PROTECTION OF TRADE SECRETS.—At the request of any party to an action brought pursuant to this subsection or any other participant in such an action, the court may, in its discretion, issue protective orders and conduct legal proceedings in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer program, and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any such party or participant.

(c) ENFORCEMENT BY STATES.—

(1) IN GENERAL.—

(A) CIVIL ACTIONS.—In any case in which the attorney general 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 the engagement of any person in a practice that violates section 5 of this Act, the State may bring civil action on behalf of the residents of the State in an appropriate court of that State, or in a district court of the United States of appropriate jurisdiction for any or all of the following relief:

(i) INJUNCTION.—To enjoin that practice.

(ii) COMPLIANCE ENFORCEMENT.—To enforce compliance with the provisions of section 5.

(iii) DAMAGES.—To recover actual monetary loss or receive $500 in damages for each violation, except that if the court finds that the defendant willfully or repeatedly violated section 5, the court may, in its

discretion, increase the amount of the award to an amount equal to not more than 3 times the amount otherwise available under this clause.

(B) LIMITATION ON MONETARY DAMAGES.—All monetary amounts recovered or received by settlement or judgment in an action under this paragraph shall be paid directly to the persons who incurred losses or suffered damages as a result of the violation under section 5 for which the action was brought, and no such amounts may be retained by the State or may be used directly or indirectly to offset the cost of such litigation.

(C) NOTICE.—

(i) IN GENERAL.—Before filing an action under subparagraph (A), the attorney general of the State involved shall provide to the Commission—

(I) written notice of that action; and

(II) a copy of the complaint for that action.

(ii) EXEMPTION.—

(I) IN GENERAL.—Clause (i) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general determines that it is not feasible to provide the notice described in that subparagraph before the filing of the action.

(II) NOTIFICATION.—In an action described in subclause (I), the attorney general of a State shall provide notice and a copy of the complaint to the Commission at the same time as the attorney general files the action.

(2) INTERVENTION.—

(A) IN GENERAL.—On receiving notice under paragraph (1)(B), the Commission shall have the right to intervene in the action that is the subject of the notice.

(B) EFFECT OF INTERVENTION.—If the Commission intervenes in an action under paragraph (1), it shall have the right—

(i) to be heard with respect to any matter that arises in that action; and

(ii) to file a petition for appeal.

(3) 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.

(4) 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) may be found.

SEC. 7. EFFECT ON OTHER LAWS.

(a) FEDERAL LAW.—Nothing in this Act shall be construed to impair the enforcement of section 223 or 231 of the Communications Act of 1934, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code, or any other Federal criminal law or any State criminal law regarding obscenity or the sexual exploitation of children.

(b) STATE LAW.—No State or local government may impose any civil liability for commercial activities or actions in interstate or foreign commerce in connection with an activity or action described in section 5 of this Act that is inconsistent with the treatment of such activities or actions under this Act, except that this Act shall not preempt any civil action under—

(1) State trespass or contract law; or

(2) any provision of Federal, State, or local criminal law or any civil remedy available under such law that relates to acts of computer fraud or abuse arising from the unauthorized transmission of unsolicited commercial electronic mail messages.

SEC. 8. STUDY OF EFFECTS OF UNSOLICITED COMMERCIAL ELECTRONIC MAIL.

Not later than 18 months after the date of the enactment of this Act, the Federal Trade Commission 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.

SEC. 9. SEVERABILITY.

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. 10. EFFECTIVE DATE.

The provisions of this Act shall take effect 60 days after the date of the enactment of this Act.

PURPOSE AND SUMMARY

The purpose of H.R. 718, the Unsolicited Commercial Electronic Mail Act of 2001, is to prohibit the initiation and transmission of unsolicited commercial electronic mail messages. The legislation is narrowly drawn to protect freedom of speech on the Internet and legitimate commercial uses of electronic mail messages.

H.R. 718 prohibits the transmission of unsolicited commercial electronic mail messages unless the initiator of such message provides a valid electronic mail return address and provides the recipient of such messages the opportunity not to receive future mailings. In addition, the bill allows Internet access service providers (ISP) to decline further unsolicited commercial electronic mail (UCE) messages, if the ISP has a policy of no UCE or the ISP has received a significant number of complaints from its customers. Under H.R. 718, the Federal Trade Commission is authorized to enforce the Act. Further, State or local laws that are inconsistent with the Act are preempted, except in the case of any civil remedy under State trespass or contract law, any State or local law relating to acts of computer fraud and abuse arising from the unauthorized transmission of unsolicited commercial electronic mail messages, or any State criminal law regarding obscenity or risk of injury to children.

BACKGROUND AND NEED FOR LEGISLATION

The creation and growth of the Internet has been one of the most important developments of the second half of the 20th century. From its origin as an academic research tool in the 1960's, the Internet has become today a global communications, information, entertainment and commercial medium.

The use of the Internet to conduct commercial activities, often referred to as "electronic commerce," has experienced enormous growth. In 1996, consumers spent just $2.6 billion in online transactions, compared to more than $50 billion in 1999. Because of significant efficiencies gained from electronic transactions and the enormous reach of the Internet, the Internet is now used to supplement, or in some cases replace, traditional commercial methods.

In one area, the sending of electronic commercial solicitations (either requested or not requested by a consumer), the Internet has brought tremendous efficiencies of scale. Unlike traditional commercial solicitations delivered via the postal system, the marginal cost of electronic solicitations approaches zero.

Given its ability to quickly disseminate multiple electronic messages, the Internet has heightened consumer anxiety over unwanted commercial solicitations. This has led many consumer groups to ask Congress and the States to enact restrictions on un-

solicited commercial electronic (UCE) mail messages, more commonly known as "spam."

There are a number of consumer concerns regarding unsolicited commercial electronic mail messages. First, a substantial portion of those messages contains solicitations that are false or misleading. In discussing the use of unsolicited commercial electronic mail messages to mislead consumers, Eileen Harrington, the Associate Director of Marketing Practices at the Federal Trade Commission testified that:

> * * * UCE has become the fraud artists's calling card on the Internet. Much of the spam in the Commissions's database contain false information about the sender, misleading subject lines, and extravagant earnings or performance claims about goods and services. These types of claims are the stock in trade of fraudulent schemes. * * * The Commission believes the proliferation of deceptive bulk UCE on the Internet poses a threat to consumer confidence in online commerce and thus views the problem of deception as a significant issue in the debate over UCE.

(Written testimony at the November 3, 1999 hearing before the Subcommittee on Telecommunications, Trade and Consumer Protection, Serial No. 106–84, pp. 25–26.)

There are also concerns that many unsolicited commercial electronic mail messages contain material of an adult nature that can be easily accessed by children from the family computer, and in many instances these mail messages are intentionally sent with incorrect routing information.

The issue of unsolicited commercial advertisements has been the subject of much debate in the United States over the past decades. From in-person solicitations, phone-based telemarketing, junk-faxes, and now Internet-based solicitations, consumers have historically complained that these unwanted solicitations are an incredible nuisance.

In 1991, Congress passed the Telephone Consumer Protection Act (P.L. 102–243) to restrict the use of automated, pre-recorded telephone calls and unsolicited commercial fax transmissions. Congress found such unsolicited faxes and automated telephone calls were a nuisance and an invasion of privacy. The constitutionality of the Telephone Consumer Protection Act was upheld in *Destination Ventures Ltd.* v. *FCC*, 46 F.3d 54 (9th Cir. 1995), and *Moser* v. *FCC*, 46 F.3d 970 (9th Cir. 1995), *cert denied*, 515 U.S. 1161. In these cases, the courts concluded that Congress had accurately identified automated telemarketing calls as a threat to privacy (46 F.3d at 974) and that the banning of unsolicited commercial fax solicitations was a reasonable means of reducing cost shifting (46 F.3d at 56).

There is also concern about the burden bulk unsolicited commercial electronic mail messages place on the Internet infrastructure and on companies providing Internet access services. Unlike traditional commercial solicitations made by mail, the cost of unsolicited commercial electronic mail messages is shifted from the sender to the recipient and the recipient's ISP.

Most ISPs claim to incur significant costs from unsolicited commercial electronic mail messages, such as the costs involved with

network bandwidth, processing electronic mail, and staff time. ISPs must also address the ongoing relationship with its customers and its reputation in the marketplace for fostering an environment where spamming is prevalent. In response, many ISPs have enacted spamming policies to affect the level of blame (or credit) that is attributed to them regarding the unsolicited electronic mails their customers receive.

Generally, these laws prohibit the transmission of bulk unsolicited commercial electronic mail messages that do not contain a label identifying the message as advertising or messages containing misleading or false routing information. Many laws also require senders of unsolicited commercial electronic mail messages to provide recipients the opportunity to opt-out of the receipt of future mailings.

HEARINGS

The Subcommittee on Telecommunications, Trade and Consumer Protection held a hearing on H.R. 3113, the Unsolicited Electronic Mail Act on November 3, 1999. The Subcommittee received testimony from the following witnesses: The Honorable Heather Wilson; The Honorable Gene Green; The Honorable Gary G. Miller; The Honorable Christopher H. Smith; Ms. Eileen Harrington, Associate Director of Marketing Practices Bureau of Consumer Protection, Federal Trade Commission; Mr. John Brown, President, iHighway.net Inc.; Mr. Alan Charles Raul, Sidley & Austin; Mr. Michael Russina, Senior Director Systems Operations, SBC Communications Inc.; Mr. Charles H. Kennedy, Morrison & Forester LLP; Mr. Jerry Cerasale, Senior Vice President, Direct Marketing Association; and, Mr. Ray Everett-Church, Chief Privacy Officer and Vice President for Public Privacy, Alladvantage.com.

COMMITTEE CONSIDERATION

On March 21, 2001, the Subcommittee on Telecommunications and the Internet met in open markup session and approved H.R. 718, the Unsolicited Electronic Mail Act of 2001 for Full Committee consideration, as amended, by a voice vote. On March 28, 2001, the Full Energy and Commerce Committee met in open markup session and ordered H.R. 718 reported to the House with a favorable recommendation, as amended, by a voice vote, a quorum being present.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto. There were no record votes taken in connection with ordering H.R. 718 reported. A motion by Mr. Tauzin to order H.R. 718 reported to the House, as amended, was agreed to by a voice vote, a quorum being present.

The following amendment was agreed to by a voice vote:

> An amendment in the nature of a substitute offered by Mrs. Wilson, No. 1, (1) provides the ISP with the option to "opt-out" of receiving unsolicited commercial electronic

mail if: (a) they have a publicly available policy against receiving unsolicited commercial electronic mail and make a good faith effort to block it, or (b) a significant portion of its customer base complains to the ISP about receiving the spam, (2) clarifies that the initiator must be the actual person that "originates" the message to address ISPs that may facilitate e-mail lists, (3) defines how corporate affiliate relationships will be treated, (4) clarifies that opting out of unsolicited commercial electronic mail does not "terminate" the business relationship, (5) gives marketers a reasonable amount of time to suppress the names of consumers opting out of spam, (6) deletes notification process by Federal Trade Commission (FTC) to alleged spammer, (7) allows FTC to enforce and seek redress under the process they currently use under the Fair and Deceptive Practices Act, (8) prohibits the damages received from a State Attorney General case from going to anyone but the aggrieved plaintiffs, including to fund the litigation costs or for other state programs, (9) explicitly prohibits the FTC from promulgating any rules under this Act, (10) retains explicit prohibition against Class Actions, and (11) does not preempt a state's ability to enforce any law regarding obscenity or the sexual exploitation of children was agreed to by a voice vote.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held a legislative hearing and made findings that are reflected in this report.

PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the Committee finds that this legislation does not authorize funding, and therefore no statement is required.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 718, the Unsolicited Electronic Mail Act of 2001, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

COMMITTEE COST ESTIMATE, CONGRESSIONAL BUDGET OFFICE ESTIMATE, AND FEDERAL MANDATES STATEMENT

The Congressional Budget Office estimate required pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives section 402 of the Congressional Budget Act of 1974, and the estimate of Federal mandates required pursuant to section 423 of the Unfunded Mandates Reform Act were requested from the Congressional Budget Office, but were not prepared as of the date of filing of this report. The Congressional Budget Office estimate and

accompanying materials will be contained in a supplemental report.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause 3, which grants Congress the power to regulate commerce with foreign nations, among the several States, and with the Indian tribes.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

Section 1 establishes the short title of this Act as the "Unsolicited Commercial Electronic Mail Act of 2001. "

Section 2. Congressional findings and policies

Section 2 lays out Congressional findings and general policy on the issue of unsolicited commercial electronic mail.

Section 3. Definitions

Section 3 defines the following terms: "affiliate," "children," "commercial electronic mail message," "Commission," "domain name," "electronic mail address," "FTC Act," "initiate," "initiator," "Internet," "Internet access service," "recipient consent," "pre-existing business relationship," "recipient," and "unsolicited commercial electronic mail message."

The definition of affiliate requires both that (1) different entities are controlled by, or under common control and (2) that the entity provides marketing information to, receives marketing information from, or shares marketing information with the other entity under common control. Affiliates are included within the definition of pre-existing business relationship. As a result, if an entity has a pre-existing business relationship with an individual, then any electronic mail from an affiliate of that entity would not be considered Unsolicited Commercial Electronic Mail.

The concept of unsolicited commercial electronic mail plays a key role in the understanding of H.R. 718. As used in the bill, the term unsolicited commercial electronic mail means any commercial electronic mail message sent to an individual with whom the initiator of the electronic message does not have prior recipient consent and does not have a pre-existing business relationship. The Committee wants to clarify that a request by a recipient of commercial electronic mail to not receive further messages from the initiator and

any affiliates of the initiator does not terminate the business relationship between the initiator and the recipient. In particular, the Committee does not wish to limit e-commerce between the initiator and recipient for renewal, upgrade or replacement of existing service provided by the initiator. In addition, electronic mails concerning billing and legal notices shall not constitute unsolicited commercial electronic mail messages.

The Committee changed an element of the definition of "initiator" contained in the Subcommittee passed bill from "a message composed and addressed by others" to "a message originated by others" in an effort to make clear that only the sender of the message is culpable, rather than companies the sender may utilize to get the message to the end user. When these intermediary companies do not select the lists that are used, nor make the decision that the message should be sent to a given list of recipients, they should not be considered to have originated the message. For example, even if an ISP plays a role in facilitating an agreement between a list broker and a company wishing to get a message out, it should not be liable for any illegal message, unless it actually originates the message. The Committee wants to clarify that ISPs will not fall into the definition of initiator when acting in capacities such as the transmission, routing, relaying, handling, or storing, through an automatic technical process, as long as the ISP is not originating the message.

If an initiator has a pre-existing business relationship with a recipient and the recipient requests not to receive further commercial electronic mail messages, such a request would apply only to subsequent messages that advertise or promote the commercial availability of a product or service for profit. Such a request would not apply to the sending of messages for billing, administrative, legal compliance, or other communications whose primary purpose is not to advertise or promote the commercial availability of a product or service for profit.

Section 4. Criminal penalty for unsolicited commercial electronic mail containing fraudulent routing information

Section 4 amends Section 1030 of Title 18 of the United States Code, which encompasses fraud and related activity in connection with computers. Section 4 of this Act will add a paragraph to the end of subsection (a)(5) of Section 1030 of Title 18 of the US Code. The paragraph states that if any person intentionally initiates the transmission of unsolicited commercial electronic mail with knowledge that any identifying information of the initiator or routing information is false, such person will be punishable under criminal law. A violation of this amendment to the Title 18 of the US Code will result in a fine or imprisonment of not more than one year, or both.

Section 5. Other protections against unsolicited commercial electronic mail

Section 5(a)(1) provides that it is unlawful for any person to initiate the transmission of an unsolicited commercial electronic mail message to any person within the United States unless that message contains a valid, conspicuously displayed electronic mail ad-

dress to which a recipient may reply requesting not to receive any further messages.

Section 5(a)(2) prohibits the transmission of an unsolicited commercial electronic mail message by the person or any affiliates of such person after the expiration of a reasonable period of time for removal from such lists. After such request is made, such person and affiliates must delete or suppress the electronic mail addresses of the recipient from all mailing lists owned or controlled by such person or affiliate within a reasonable period of time for such deletion or suppression. Further, it shall be unlawful for such person or affiliate to sell, lease, exchange, license or engage in any other transaction involving the mailing lists with the recipient's electronic mail address. The Committee intended for it to become standard practice in marketing and other industries to honor such requests by maintaining a list of individuals that have opted-out of the receipt of unsolicited commercial electronic mail. Such lists should suppress these electronic mail addresses from further solicitation.

Section 5(a)(3) prohibits the transmission of unsolicited commercial electronic mail messages that do not contain a clear and conspicuous identification that the message is unsolicited commercial electronic mail, notice of an opportunity to decline to receive further unsolicited commercial electronic mail, and the physical mailing address of the initiator.

Section 5(a)(4) provides that if an ISP requires compensation specifically for the transmission of unsolicited commercial electronic mail messages into its system, the provider must provide an option to its subscribers not to receive any unsolicited commercial electronic mail messages, except that such option is not required for any subscriber who has agreed to receive unsolicited commercial electronic mail messages in exchange for discounted or free Internet access service. The Committee intends an ISP must receive compensation specifically for transmission of unsolicited commercial electronic mail messages, not merely compensation for the transmission of any electronic mail messages, whether commercial or non-commercial or solicited or unsolicited.

Section 5(a)(5) states that it shall be an affirmative defense that an alleged violation of any paragraph of this subsection was not intentional.

Section 5(b) provides the conditions for enforcement by providers of Internet access service. Opt-out by ISPs is limited to those Internet access services that directly provide service to a recipient of electronic mail messages. Electronic mail messages typically may cross several Internet access services networks, often without the knowledge of the initiator, before reaching their destination. Because the initiator would have no means of determining the path an electronic mail message takes on route to the recipient, the opt-out for purposes of section 5(b) applies only to equipment of the ISP that delivers messages directly to a recipient.

Section 5(b)(1) prohibits any person from transmitting an unsolicited commercial electronic mail message to any ISP in violation of its policy regarding unsolicited commercial electronic mail messages. In order to take advantage of this provision, the ISP must either (1) adopt a policy that complies with the requirements of section 5(b)(2), or (2) receive a significant number of complaints from

its bona fide subscribers regarding unsolicited commercial electronic mail from such person. In either case, the initiator is given a reasonable period of time to comply with an ISP request not to receive further unsolicited commercial electronic messages.

Section 5(b)(2) establishes the requirements for an ISP policy regarding unsolicited commercial electronic mail messages. The policy must explicitly prohibit unsolicited commercial electronic mail; the ISP must make a good faith effort to block the transmission of all unsolicited commercial electronic mail, the policy must be publicly available by the clear and conspicuous posting on a World Wide Web site with an Internet domain name that is identical to that of the prohibited electronic mail address, and the ISP informs each subscriber about its policy.

Section 5(c)(1) clarifies that nothing in H.R. 718 is to be construed to prevent or limit, in any way, a provider of Internet access service from adopting a policy regarding commercial or other electronic mail and from enforcing this policy through technical means, contract or any remedy available under any other provision of Federal, State, or local criminal or civil law.

Section 5(c)(2) clarifies that nothing in H.R. 718 renders lawful and such policy that is unlawful under any other provision of law.

Section 5(d) provides that a provider of Internet access service is not to be liable, under any Federal, State, or local civil or criminal law, for any action it takes in good faith to block the transmission or receipt of unsolicited commercial electronic mail messages that are sent in violation of this section. The Committee notes that section 5 is intended to primarily establish the unlawfulness of certain acts by initiators of unsolicited commercial electronic mail, remedies for which are provided in section 6 to the FTC, State Attorneys General, ISPs, and recipients. ISPs may elect not to use these remedies for a variety of reasons but, with the exception of a narrow provision in paragraph (a)(4), section 5 is not intended for use as an enforcement or remedial tool against ISPs, and does not create any cause of action against an ISP. Neither shall it be used as an affirmative defense to any cause of action brought by an ISP other than provided for in Section 5(a)(5).

Section 6. Enforcement

Section 6(a)(1) provides for enforcement of Section 5 of the Act by the FTC under the FTC Act.

Section 6(a)(2) states that any violation of section 5 shall be treated as a violation of section 18 of the FTC Act regarding unfair or deceptive acts or practices.

Section 6(a)(3) states that the scope of the Commission's enforcement of Section 5 of this Act will be the same manner in which they enforce similar violations under the FTC Act.

Section 6(a)(4) provides for a prohibition of the Commission or any other Federal agency to issue any regulations in order to implement this Act. This act does not affect the existing authority of the FTC or other Federal agencies to issue regulations otherwise permitted by law.

Section 6(b) creates a limited private right of action for individuals to recover actual or statutory damages associated with receiving unsolicited commercial electronic mail. The Committee intends that private actions under this section be treated as small claims

best resolved in State courts designed to handle them, which would allow injured consumers to settle claims quickly without incurring attorneys' fees. The Committee is concerned that in some instances, class action lawsuits may result in injured parties not receiving the maximum compensation possible. For this reason, section 6(b) establishes that no private action created under this section may be brought as a class action.

Section 6(b)(1) provides that a recipient or a provider of Internet access service may, if otherwise permitted by the laws or rules of court of a State, bring in an appropriate court of that State, or may bring in an appropriate Federal court if such laws or rules do not so permit, (1) an action based on a violation of section 5 to enjoin such violation, and/or (2) an action to recover for actual monetary loss from such a violation in an amount equal to the greater of the amount of such actual monetary loss or $500 for each such violation, not to exceed a total of $50,000.

Section 6(b)(2) provides that if the court finds that the defendant willfully or repeatedly violated section 4, the court may, in its discretion, increase the amount of the award to an amount equal to not more than three times the amount available under section 6(b)(1).

Section 6(b)(3) provides that in any such action, 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.

Section 6(b)(4) states that a private action that arises under this subsection may not be brought as a plaintiff class action suit under the Federal Rules of civil procedure nor as a class action pursuant to the laws or rules of procedure of any State.

Section 6(b)(5) provides that at the request of any party to an action, or any other participant in such an action, the court may, in its discretion, issue protective orders and conduct legal proceedings in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer program, and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect trade secrets of any party or participant.

Section 6(c)(1) provides for limited enforcement of the Act by the States. A State may bring an action for relief of violations of Section 5 of the Act on behalf of residents of the State subject to certain limitations.

Section 6(c)(1)(B) expressly bars the State from keeping any of the proceeds of any settlement or judgment under such an action. The Committee intends this requirement to ensure, first, that injured parties are made whole without deduction for attorneys' fees and, second, that the State will not have its own economic interest at stake in the outcome of the litigation. In addition, section 6(c)(1)(B) expressly bars a State from using funds related to a settlement or judgment to directly or indirectly offset the costs of litigation. The Committee intends the term "all monetary amounts recovered or received by settlement or judgment" should include any direct or indirect payment by the State or any other party or its counsel or agents to an opposing party or its counsel or agents.

Section 6(c)(1)(C) requires a State to provide notice to the Commission of its intent to file an action under the Act.

Section 6(c)(1)(C)(2) allows the Commission to intervene in an action that is subject to the above-referenced notice.

Section 7. Effect on other laws

Section 7(a) clarifies that nothing in this Act is to be construed to impair the enforcement of section 223 or 231 of the Telecommunications Act of 1934, 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 or any State law regarding obscenity or the sexual exploitation of children.

Section 7(b) provides that no State or local government may impose any civil liability for commercial activities or actions in interstate or foreign commerce in connection with the sending of an unsolicited commercial electronic mail message that is inconsistent with the treatment of such activities or actions under the bill. However, this Act does not preempt any civil remedy under State trespass or contract law, any provision of Federal, State, or local criminal law, or any civil remedy that relates to acts of computer fraud or abuse arising from the unauthorized transmission of unsolicited commercial electronic mail messages.

Section 8. Study of effects of unsolicited commercial electronic mail

The Federal Trade Commission is directed, within 18 months after enactment, to submit a report to 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.

Section 9. Severability

Section 8 provides a severability clause.

Section 10. Effective date

The effective date of the bill is 60 days after the date of enactment.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

SECTION 1030 OF TITLE 18, UNITED STATES CODE

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—

(1) * * *

* * * * * * *

(5)(A) * * *

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; [or]

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; *or*

(D) intentionally initiates the transmission of any unsolicited commercial electronic mail message to a protected computer in the United States with knowledge that any domain name, header information, date or time stamp, originating electronic mail address, or other information identifying the initiator or the routing of such message, that is contained in or accompanies such message, is false or inaccurate;

* * * * * * *

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1) * * *

(2)(A) a fine under this title or imprisonment for not more than one year, or both, in the case of *(i)* an offense under subsection (a)(2), (a)(3), (a)(5)(C), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph*, or (ii) an offense under subsection (a)(5)(D) of this section*; and

* * * * * * *

(e) As used in this section—

(1) * * *

* * * * * * *

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information, that—

(A) * * *

* * * * * * *

(D) threatens public health or safety; **[**and**]**

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country**[**.**]***; and*

(10) the terms "initiate", "initiator", "unsolicited commercial electronic mail message", and "domain name" have the meanings given such terms in section 3 of the Unsolicited Commercial Electronic Mail Act of 2001.

* * * * * * *

ADDITIONAL VIEWS BY HON. JOHN D. DINGELL

I believe H.R. 718 will go a long way toward eliminating the insidious problem on the Internet known as "spam."

There are some who urged this Committee to make certain changes that I believe would have seriously impaired the effectiveness of this anti-spam legislation. I am pleased those efforts to eviscerate key parts of the bill have been rejected by the bill's sponsors, Ms. Wilson and Mr. Green.

Spam is no longer a mere nuisance to the 160 million Americans now using the Internet. It has rapidly degenerated into an abusive marketing practice. Innocent users are constantly bombarded with unsolicited commercial messages over which they have no control. Worse, many of these messages are pornographic in nature, and include "teaser" images inviting the recipient to visit one adult site on the Web or another. For many families, these spam messages are more than an intrusion, they are a personal assault.

Spam also imposes real economic costs on the public. Some users pay metered charges for Internet access; others, particularly in rural areas, pay long distance telephone charges when dialing-up to the Internet. The time spent downloading unwanted messages translates into real dollars and cents. And, of course, the slower the Internet connection, the greater the tab.

Perhaps the greatest cost associated with spam is incurred by the more than 3,000 Internet Service Providers, or ISPs, in this country. These companies have little choice but to expand their server capacity to deal with the proliferation of spam. Most of these ISPs are small businesses that simply cannot afford the additional investment required. Some resort to self-help methods to delete large volumes of bulk e-mail, but this labor-intensive process is also expensive and, unfortunately, not very effective.

H.R. 718 contains several means to eliminate the problem of spam, including an opt-out for individual consumers. Unfortunately, consumers could spend most of their waking hours sending opt-out requests and still not reach every spammer on the Internet.

In my view, the most effective way to eradicate the Internet of abusive spammers is to put the matter squarely in the hands of ISPs, and this bill provides tools for ISPs to deal with the problem directly. ISPs have a direct and compelling financial incentive to protect both the integrity of their networks and the quality of service provided to their customers.

Section 5(b) of this legislation gives ISPs, in addition to individual consumers, the right to opt-out of receiving spam. No longer will ISPs have to struggle in vain to rid themselves of unwanted spam that is clogging their networks and infuriating their customers. They can elect to opt-out of spam, and enforce that policy against violators. In my view, it is a critical element contained in

this legislation to protect consumers, once and for all, from the increasing struggle against this offensive practice.

Just as important, the bill preserves a right already available to ISPs under existing law. Section 5(c) permits ISPs to continue using defensive measures, technical and otherwise, to block the unwanted messages that overload their networks and outrage their customers.

The bill also contains important enforcement measures. It affords individuals and ISPs a private right of action against spammers who do not comply. It also empowers the Federal Trade Commission to enforce the bill's anti-spamming provisions, and carries steep penalties for violators.

I would note, however, that an important enforcement mechanism contained in the Subcommittee-passed bill was weakened when the bill was considered by the full Committee, and is the cause of some concern. The Subcommittee originally agreed on a compromise that prohibited class action lawsuits, and instead authorized State Attorneys General to enforce the bill's anti-spam provisions on behalf of aggrieved citizens in their respective States. Unfortunately, an amendment at full Committee had the effect of weakening the State AGs' ability to pursue wrongdoers by expressly prohibiting the recovery of any litigation costs associated with an enforcement action.

In my view, it is simply unfair to require the taxpaying public to foot the legal bill for the damage caused by spammers. Recovery of reasonable legal fees is properly included in damage awards to individuals under this bill, and I believe it should likewise be permitted when the State acts as an agent on their behalf. If we are serious about putting an end to spam, as I hope we are, then we should not be creating a disincentive to enforcing the law against it.

On balance, the bill is a good one, and I was happy to support it. However, it is imperative that further attempts to weaken the bill's enforcement provisions are rejected as this bill moves to the House Floor and thereafter.

JOHN D. DINGELL.

○