106TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
106–700

UNSOLICITED COMMERCIAL ELECTRONIC MAIL ACT OF 2000

JUNE 26, 2000.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. BLILEY, from the Committee on Commerce, submitted the following

REPORT

[To accompany H.R. 3113]

[Including cost estimate of the Congressional Budget Office]

The Committee on Commerce, to whom was referred the bill (H.R. 3113) 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

79–006

AMENDMENT

The amendment is as follows:

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 2000".

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) 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.

(2) 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.

(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.—

(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").

(6) 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)).

(7) 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)).

(8) INITIATE.—The term "initiate", when used with respect to a commercial electronic mail message, means to originate such message or to procure the transmission 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 whose role is limited to handling, transmitting, or retransmitting the message.

(10) 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 either of the following circumstances exist:

(A) PREVIOUS BUSINESS TRANSACTION.—

(i) Within the 5-year period ending upon receipt of such message, there has been a business transaction between the initiator and the recipient (including a transaction involving the provision, free of charge, of information requested by the recipient, of goods, or of services); and

(ii) the recipient was, at the time of such transaction or thereafter, provided a clear and conspicuous notice of an opportunity not to receive further messages from the initiator and has not exercised such opportunity.

(B) OPT IN.—The recipient has given the initiator permission to initiate commercial electronic mail messages to the electronic mail address of the recipient and has not subsequently revoked such permission.

(11) RECIPIENT.—The term "recipient", when used with respect to a commercial electronic mail message, means the addressee of such message.

(12) UNSOLICITED COMMERCIAL ELECTRONIC MAIL MESSAGE.—The term "unsolicited commercial electronic mail message" means any commercial electronic mail message that is sent by the initiator to a recipient with whom the initiator does not have a pre-existing business relationship.

SEC. 4. PROTECTIONS AGAINST UNSOLICITED COMMERCIAL ELECTRONIC MAIL.

(a) REQUIREMENTS FOR TRANSMISSION OF MESSAGES.—

(1) INCLUSION OF RETURN ADDRESS.—It shall be unlawful for any person to initiate the transmission of an unsolicited 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.

(2) PROHIBITION OF TRANSMISSION AFTER OBJECTION.—If a recipient makes a request to a person to be removed from all distribution lists under the control of such person, it shall be unlawful for such person to initiate the transmission of an unsolicited commercial electronic mail message to such a recipient within the United States after the expiration, after receipt of such request, of a reasonable period of time for removal from such lists. Such a request shall be deemed

to terminate a pre-existing business relationship for purposes of determining whether subsequent messages are unsolicited commercial electronic mail messages.

(3) ACCURATE ROUTING INFORMATION.—It shall be unlawful for any person who initiates the transmission of any unsolicited commercial electronic mail message to any person within the United States to take any action that causes any Internet routing information contained in or accompanying such message—

(A) to be inaccurate;

(B) to be invalid according to the prevailing standards for Internet protocols; or

(C) to fail to accurately reflect the routing of such message.

(4) INCLUSION OF IDENTIFIER AND OPT-OUT.—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; and

(B) notice of the opportunity under paragraph (2) not to receive further unsolicited commercial electronic mail messages from the initiator.

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

(1) AUTHORITY TO ESTABLISH POLICIES.—A provider of Internet access service may enforce a policy regarding unsolicited commercial electronic mail messages, but only if such policy complies with the requirements of paragraph (3).

(2) PROHIBITION OF TRANSMISSIONS IN VIOLATION OF POSTED POLICY.—It shall be unlawful for any person to initiate the transmission of an unsolicited commercial electronic mail message to any person within the United States in violation of a policy governing the use of the equipment of a provider of Internet access service for transmission of unsolicited commercial electronic mail messages that meets the requirements of paragraph (3).

(3) REQUIREMENTS FOR ENFORCEABILITY.—The requirements under this paragraph for a policy regarding unsolicited commercial electronic mail messages are as follows:

(A) CLARITY.—The policy shall explicitly provide that compliance with a rule or set of rules is a condition of use of the equipment of a provider of Internet access service to deliver commercial electronic mail messages.

(B) PUBLICLY AVAILABILITY.—The policy shall be publicly available by at least one of the following methods:

(i) WEB POSTING.—The policy is clearly and conspicuously posted 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 rule or set of rules applies.

(ii) NOTIFICATION IN COMPLIANCE WITH TECHNOLOGICAL STANDARD.—Such policy is made publicly available by the provider of Internet access service in accordance with a technological standard adopted by an appropriate Internet standards setting body (such as the Internet Engineering Task Force) and recognized by the Commission by rule as a fair standard.

(C) INTERNAL OPT-OUT LIST.—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, the provider shall 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.

(4) OTHER ENFORCEMENT.—Nothing in this Act shall be construed to prevent or limit, in any way, a provider of Internet access service from enforcing, pursuant to any remedy available under any other provision of Federal, State, or local criminal or civil law, a policy regarding unsolicited commercial electronic mail messages that complies with the requirements of paragraph (3).

(c) PROTECTION OF INTERNET ACCESS SERVICE PROVIDERS.—

(1) 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.

(2) INNOCENT RETRANSMISSION.—A provider of Internet access service the facilities of which are used only as an intermediary, retransmitter, or relay for unsolicited bulk commercial electronic mail messages transmitted in violation of subsection (a) shall not be liable for any harm resulting from the trans-

mission or receipt of such electronic mail unless it permits the transmission or retransmission of such electronic mail with actual knowledge that the transmission is prohibited by subsection (a) or subsection (b)(2).

SEC. 5. ENFORCEMENT.

(a) GOVERNMENTAL ORDER.—

(1) NOTIFICATION OF ALLEGED VIOLATION.—The Commission shall send a notification of alleged violation to any person who violates section 4 if—

(A) a recipient or a provider of Internet access service notifies the Commission, in such form and manner as the Commission shall determine, that a transmission has been received in violation of section 4; or

(B) the Commission has other reason to believe that such person has violated or is violating section 4.

(2) TERMS OF NOTIFICATION.—A notification of alleged violation shall—

(A) identify the violation for which the notification was issued;

(B) direct the initiator to refrain from further violations of section 4;

(C) expressly prohibit the initiator (and the agents or assigns of the initiator) from further initiating unsolicited commercial electronic mail messages in violation of section 4 to the designated recipients or providers of Internet access service, effective on the 3rd day (excluding Saturdays, Sundays, and legal public holidays) after receipt of the notification; and

(D) direct the initiator (and the agents or assigns of the initiator) to delete immediately the names and electronic mail addresses of the designated recipients or providers from all mailing lists owned or controlled by the initiator (or such agents or assigns) and prohibit the initiator (and such agents or assigns) from the sale, lease, exchange, license, or other transaction involving mailing lists bearing the names and electronic mail addresses of the designated recipients or providers.

(3) COVERAGE OF MINOR CHILDREN BY NOTIFICATION.—Upon request of a recipient of an electronic mail message transmitted in violation of section 4, the Commission shall include in the notification of alleged violation the names and electronic mail addresses of any child of the recipient.

(4) ENFORCEMENT OF NOTIFICATION TERMS.—

(A) COMPLAINT.—If the Commission believes that the initiator (or the agents or assigns of the initiator) has failed to comply with the terms of a notification issued under this subsection, the Commission shall serve upon the initiator (or such agents or assigns), by registered or certified mail, a complaint stating the reasons for its belief and request that any response thereto be filed in writing with the Commission within 15 days after the date of such service.

(B) HEARING AND ORDER.—If the Commission, after an opportunity for a hearing on the record, determines that the person upon whom the complaint was served violated the terms of the notification, the Commission shall issue an order directing that person to comply with the terms of the notification.

(C) PRESUMPTION.—For purposes of a determination under subparagraph (B), receipt of any transmission in violation of a notification of alleged violation 30 days (excluding Saturdays, Sundays, and legal public holidays) or more after the effective date of the notification shall create a rebuttable presumption that such transmission was sent after such effective date.

(5) ENFORCEMENT BY COURT ORDER.—Any district court of the United States within the jurisdiction of which any transmission is sent or received in violation of a notification given under this subsection shall have jurisdiction, upon application by the Attorney General, to issue an order commanding compliance with such notification. Failure to observe such order may be punishable by the court as contempt thereof.

(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 4 to enjoin such violation.

(B) An action to recover for actual monetary loss from such a violation in an amount equal to the greatest 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, knowingly, or repeatedly violated section 4, the court may, in its discretion, in-

crease 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) 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.

SEC. 6. EFFECT ON OTHER LAWS.

(a) NO EFFECT ON CRIMINAL 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 statute.

(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 4 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 remedy under State trespass or contract law or under 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. 7. STUDY OF EFFECTS OF UNSOLICITED COMMERCIAL ELECTRONIC MAIL.

Not later than 18 months after the date of enactment of this Act, the 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. 8 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. 9. EFFECTIVE DATE.

The provisions of this Act shall take effect 90 days after the date of enactment of this Act.

PURPOSE AND SUMMARY

The purpose of H.R. 3113, the Unsolicited Commercial Electronic Mail Act of 2000, is to prohibit the initiation and transmission of unsolicited commercial electronic mail messages. The legislation is narrowly drawn to protect the freedom of speech on the Internet and to protect legitimate commercial uses of electronic mail messages.

H.R. 3113 prohibits the transmission of unsolicited commercial electronic mail messages unless the initiator of that message provides a valid return electronic mail address and provides the recipient of such messages the opportunity not to receive future mailings. In addition, the bill allows Internet Service Providers (ISP) to enforce their own policy against unsolicited commercial electronic mail messages. Under H.R. 3113, the Federal Trade Commission is authorized to bring action against initiators of unsolicited commercial electronic mail messages who operate in violation of the legislation's provisions. Further, State or local laws that are inconsistent with section 4 of H.R. 3113 are preempted, except in the case of any civil remedy under State trespass or contract law or any Federal, state or local law relating to acts of computer fraud

and abuse arising from the unauthorized transmission of unsolicited commercial electronic mail messages.

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 today has become 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 the tremendous 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 in particular, 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 mail, electronic solicitations delivered via electronic mail cost almost nothing to create and transmit.

Given its ability to quickly and efficiently disseminate multiple electronic messages, the Internet has heightened consumer anxiety over unwanted commercial solicitations, and led many consumer groups to ask Congress and the States to enact restrictions on unsolicited 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 contain 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' 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, and can easily be accessed by children from the family computer.

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, to phone-based telemarketing, to junk-faxes, and now to Internet-based solicitations, consumers have historically complained that these unwanted solicitations violate their privacy.

The intrusion on an individual's privacy, and the time and financial burdens of deleting unwanted messages is the driving concern behind the proposed legislation to regulate the practice of spamming. Case law has developed the notion of "privacy rights" of recipients establishing limits on unsolicited commercial solicitations. But First Amendment rights of commercial speech to individuals who wish to receive such solicitations have led courts to find differing levels of regulation permissible, depending on the medium. In determining the appropriate level of regulation, the Court considers the amount of control individuals can exercise over the content and the medium's invasive nature.

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 that 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 e-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 e-mails their customers receive.

To date, sixteen States have enacted laws to prohibit or restrict the transmission of such messages. 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 which contain 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. This year, courts have found the anti-spam laws of California and Washington to be in violation of the Commerce Clause of the United States Constitution. Although both cases are still pending, these events show the need for this issue to be addressed by the Congress.

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 23, 2000, the Subcommittee on Telecommunications, Trade and Consumer Protection met in open markup session and approved H.R. 3113, the Unsolicited Electronic Mail Act for Full Committee consideration, amended, by a voice vote. On June 14, 2000, the Full Committee met in open markup session and ordered H.R. 3113 reported to the House, 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. 3113 reported. A motion by Mr. Bliley to order H.R. 3113 reported to the House, without amendment, 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 by Mrs. Wilson, No. 1, making various changes to the bill as approved by the Subcommittee on Telecommunications, Trade, and Consumer Protection.

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.

COMMITTEE ON GOVERNMENT REFORM OVERSIGHT FINDINGS

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, no oversight findings have been submitted to the Committee by the Committee on Government Reform.

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. 3113, the

Unsolicited Electronic Mail Act, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

COMMITTEE COST ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, June 26, 2000.

Hon. TOM BLILEY,
Chairman, Committee on Commerce,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3113, the Unsolicited Commercial Electronic Mail Act of 2000.

If your wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Ken Johnson (for federal costs), Shelley Finlayson (for the state and local impact), and Jean Wooster (for the impact on the private sector.

Sincerely,

BARRY B. ANDERSON
(For Dan L. Crippen, Director).

Enclosure.

H.R. 3113—Unsolicited Commercial Electronic Mail Act of 2000

Summary: H.R. 3113 would enact new restrictions on the transmission of unsolicited commercial electronic mail (UCE). Under this bill, consumers would have the right to file a complaint with the Federal Trade Commission (FTC) if they receive UCE after previously opting not to receive such electronic mail. Also, the bill would require that all UCE messages identify themselves as UCE, explain how the consumer could discontinue receiving UCE, and contain accurate information about the senders and how to contact them. The FTC would be required to issue compliance orders to persons who violate these provisions. H.R. 3113 also gives consumers the right to initiate private action to prohibit violations of the bill and recover damages. Finally, the bill would direct the FTC to issue a study within 18 months on the effectiveness and enforcement of these provisions.

CBO estimates that implementing H.R. 3113 would cost about $13 million in 2001 and about $60 million over the 2001–2005 period, assuming appropriation of the necessary amounts. The cost of implementing the bill could decline over time if it discourages UCE. H.R. 3113 would not affect spending or receipts; therefore, pay-as-you-go procedures would not apply.

H.R. 3113 contains intergovernmental mandates as defined in UMRA, but CBO estimates that complying with these mandates would result in no direct costs to state and local governments and thus would not exceed the threshold established by that act ($55 million in 2000, adjusted annually for inflation). The bill would preempt certain state and local laws to regulate UCE, and certain state and local liability laws. Tribal governments would not be affected.

H.R. 3113 would impose private-sector mandates, as defined by UMRA, on senders of unsolicited commercial electronic mail. CBO estimates that the direct costs of those mandates would not exceed the annual threshold established by UMRA for private-sector mandates ($109 million in 2000, adjusted for inflation).

Estimates cost to the Federal Government: The estimated budgetary impact of H.R. 3113 is shown in the following table. The costs of this legislation fall within budget function 370 (commerce and housing credit).

	By fiscal year, in millions of dollars—				
	2001	2002	2003	2004	2005
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Estimated Authorization Level	13	11	11	12	12
Estimated Outlays	13	11	11	12	12

Basis of estimate: CBO estimates that the FTC would spend about $13 million in 2001 and $11 million to $12 million annually in subsequent years to implement H.R. 3113, assuming appropriation of the necessary amounts. (Annual cost would rise slightly to cover anticipated inflation.) However, the total costs of implementing H.R. 3113 could decline if the bill is effective in reducing the amount of unlawful UCE over time.

The FTC's administrative costs would increase primarily because H.R. 1331 would require the agency to notify senders of UCE when they violate provisions of the bill. The FTC currently receives an average of about 10,000 complaints per day regarding UCE. Based on information from the FTC, CBO estimates that the staff costs of responding to these complaints would be $6 million to $7 million a year. We estimate that purchasing new computer equipment to handle UCE cases would cost $5 million in 2001 and $2 million a year in subsequent years.

For those violators who continue to send unlawful UCE after they have been notified of violations, H.R. 3113 requires that the FTC send a complaint by certified mail. CBO estimates that the cost of sending these formal complaints would be $2 million a year.

If the complaint fails to end the violations, then H.R. 3113 requires that the FTC issue an order to the violator. The FTC also has the option of referring the case to the federal courts. CBO estimates that these costs would not be significant because of the limited number of cases that would reach this stage in the enforcement process.

H.R. 3113 also requires the FTC to complete, within 18 months, a study of the effectiveness and enforcement of the bill. Based on information from the FTC, CBO estimates that the costs of this study would not be significant.

Pay-as-you-go considerations: None.

Estimated impact on state, local, and tribal governments: H.R. 3113 would preempt state and local regulation of UCE to the extent that such laws exist and conflict with this bill's requirements. In addition, the bill would preempt state and local liability laws as they apply to Internet service providers (ISPs) in certain instances. These preemptions would be intergovernmental mandates as defined in UMRA, but CBO estimates that complying with these mandates would result in no direct costs to state and local governments and thus would not exceed the threshold established in that act ($55 million in 2000, adjusted annually for inflation). Tribal governments would not be affected by these provisions.

Estimated impact on the private sector: H.R. 3113 would impose private-sector mandates as defined by UMRA on senders of UCE. The bill would require senders to identify their messages as UCE, and provide a valid return electronic-mail address and an accurate routing number within their messages. The bill also would require persons who send UCE to provide the recipients of their messages with an option to discontinue receiving UCE from the sender, and to notify recipients of that option to discontinue in each UCE message.

In addition, H.R. 3113 would make it unlawful for any person to initiate the transmission of an UCE message to any person within the United States in violation of a policy developed by an ISP governing the use of its equipment for transmission of UCE messages based on the guidelines outlined in the bill. However, this would have only a limited effect on the private sector because the Computer Fraud and Abuse Act of 1986 currently prohibits some forms of UCE transmissions. Nonetheless, it is not clear that existing federal law prohibits all transmissions of UCE in violation of an ISP policy against such transmissions.

Based on information from government and industry sources, CBO estimates that the direct costs of those mandates would not exceed the annual threshold established by UMRA for private-sector mandates ($109 million in 2000, adjusted for inflation).

Estimate prepared by Federal Costs: Ken Johnson; Impact on State, Local, and Tribal Governments: Shelly Finlayson; Impact on the Private Sector: Jean Wooster.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

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 2000."

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: "children," "commercial electronic mail message," "Commission," "domain name," "electronic mail address," "Internet," "Internet access service," "initiate," "initiator," "pre-existing business relationship," "recipient," and "unsolicited commercial electronic mail message'.

The concept of unsolicited commercial electronic mail plays a key role in the understanding of H.R. 3113. As used in the bill, the term unsolicited commercial electronic mail means any commercial electronic mail message that is sent to an individual with whom the initiator of the electronic message does not have a pre-existing business relationship.

H.R. 3113 provides for two types of business relationships that may qualify as a pre-existing business relations: (1) When there has been a business transaction between the initiator of an electronic message and the recipient in the past five years and the recipient was provided a clear and conspicuous notice of the opportunity not to receive further electronic message from the initiator and the recipient has not exercised that option, or (2) When the recipient has given permission to the initiator to send electronic mail messages and has not revoked such permission. The Committee intends that business transactions involving the provisioning of information, goods or services free of charge also qualifies as a business transaction, such as a subscription to a free Internet access service or a free newsletter.

Section 4. Protections against unsolicited commercial electronic mail

Section 4(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 address to which a recipient may reply requesting not to receive any further messages.

Section 4(a)(2) prohibits the transmission of an unsolicited commercial electronic mail message after the recipient has objected to the receipt of further unsolicited commercial electronic mail mes-

sages. A request not to receive further unsolicited commercial electronic mail messages is be deemed to terminate a pre-existing business relationship for purposes of determining whether subsequent messages are unsolicited commercial electronic mail messages.

Section 4(a)(3) prohibits the transmission of unsolicited commercial electronic mail messages that contain inaccurate or invalid routing information or any routing information that fails to accurately reflect the routing of that electronic mail message.

Section 4(a)(4) prohibits the transmission of any unsolicited commercial electronic mail message to any person within the United States unless the message clearly and conspicuously provides identification that the message is an unsolicited commercial electronic mail message and notice of the opportunity not to receive further unsolicited commercial electronic mail messages from the initiator.

Section 4(b)(1) permits a provider of Internet access service to enforce a policy regarding unsolicited commercial electronic mail messages, but only if that policy complies with the requirements of section (4)(b)(3).

Section 4(b)(2) prohibits the transmission of an unsolicited commercial electronic mail message to any person within the United States in violation of a policy governing the use of the equipment of a provider of Internet access service for transmission of unsolicited commercial electronic mail messages.

Section 4(b)(3) establishes the requirements for an Internet access provider policy regarding unsolicited commercial electronic mail messages. The requirements are—

- The policy must explicitly state that compliance with the rules is a condition of use of the equipment of a provider of Internet access service to deliver commercial electronic mail messages;
- The policy must be publicly available by the clear and conspicuous posting on a World Wide Web site of the provider of Internet access service or the policy is made publicly available by the provider of Internet access service in accordance with a technological standard adopted by an appropriate Internet standards setting body (such as the Internet Engineering Task Force) and recognized by the Federal Trade Commission by rule as a fair standard; and,
- 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, 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 that for purposes of subparagraph (C) an Internet access provider must receive compensation specifically for transmission of unsolicited commercial electronic mail messages, not merely compensation for the transmission of any mail messages, whether commercial or noncommercial or solicited or unsolicited.

Section 4(b)(4) clarifies that nothing in H.R. 3113 is to be construed to prevent or limit, in any way, a provider of Internet access service from enforcing, pursuant to any remedy available under

any other provision of Federal, State, or local criminal or civil law, a policy regarding unsolicited commercial electronic mail messages.

Section 4(c)(1) 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.

Section 4(c)(2) provides that a provider of Internet access service, whose facilities are used only as an intermediary, retransmitter, or relay for unsolicited bulk commercial electronic mail messages transmitted in violation of subsection (a), is not to be liable for any harm resulting from the transmission or receipt of such electronic mail unless it permits the transmission or retransmission of such electronic mail with actual knowledge that the transmission is prohibited.

Section 5. Enforcement

Under section 5(a)(1) of the bill, the Federal Trade Commission (the Commission) is to send a notification of alleged violation to any person who violates section 4 if: (1) a recipient or a provider of Internet access service notifies the Commission (in a for and manner as determined by the Commission) that a transmission has been received in violation of section 4, or (2) the Commission has other reason to believe that such person has violated or is violating section 4.

Section 5(a)(2) requires a notification of alleged violation to: (1) identify the violation for which the notification was issued, (2) direct the initiator to refrain from further violations of section 4, (3) expressly prohibit the initiator (and the agents or assigns of the initiator) from further initiating unsolicited commercial electronic mail messages in violation of section 4 to the designated recipients or providers of Internet access service, effective on the 3rd day (excluding Saturdays, Sundays, and legal public holidays) after receipt of the notification, and (4) direct the initiator (and the agents or assigns of the initiator) to delete immediately the names and electronic mail addresses of the designated recipients or providers from all mailing lists owned or controlled by the initiator (or such agents or assigns) and prohibit the initiator (and such agents or assigns) from the sale, lease, exchange, license, or other transaction involving mailing lists bearing the names and electronic mail addresses of the designated recipients or providers.

Section 5(a)(3) provides that upon request of a recipient of an electronic mail message transmitted in violation of section 4, the Commission must include in the notification of alleged violation the names and electronic mail addresses of any child of the recipient.

Section 5(a)(4) provides that if the Commission believes that the initiator (or an agent or assign of the initiator) has failed to comply with the terms of a notification issued under this subsection, the Commission shall serve upon the initiator (or such agents or assigns), by registered or certified mail, a complaint stating the reasons for its belief and request that any response be filed in writing with the Commission within 15 days. Further, if the Commission, after an opportunity for a hearing on the record, determines that the person upon whom the complaint was served violated the terms of the notification, the Commission must issue an order directing

that person to comply with the terms of the notification. For purposes of a determination under subparagraph (B), receipt of any transmission in violation of a notification of alleged violation 30 days (excluding Saturdays, Sundays, and legal public holidays) or more after the effective date of the notification creates a rebuttable presumption that such transmission was sent after such effective date.

Section 5(a)(5) provides that any district court of the United States within the jurisdiction of which any transmission is sent or received in violation of a notification given under this subsection has jurisdiction, upon application by the Attorney General, to issue an order commanding compliance with such notification. Failure to observe that order may be punishable by the court as contempt.

Section 5(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 4 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 greatest of the amount of such actual monetary loss or $500 for each such violation, not to exceed a total of $50,000.

Section 5(b)(2) provides that if the court finds that the defendant willfully, knowingly, 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 5(b)(1).

Section 5(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 5(b)(4) 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 any trade secrets of any such party or participant.

Section 6. Effect on other laws

Section 6(a) clarifies that nothing in this is to 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 statute.

Section 6(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 or under any provision of Federal, State, or local criminal law or any civil remedy that relates to acts of com-

puter fraud or abuse arising from the unauthorized transmission of unsolicited commercial electronic mail messages.

Section 7. 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 8. Separability

Section 8 provides a separability clause.

Section 9. Effective date

The effective date of the bill is 90 days after the date of enactment.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation does not amend any existing Federal statute.

○

DOCUMENT NO. 52