STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. VOINOVICH:

S. 1326. A bill to establish the position of Assistant Secretary of Commerce for Manufacturing in the Department of Commerce; to the Committee on Commerce, Science, and Transportation.

Mr. VOINOVICH. Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the bill was ordered to be printed in the RECORD, as follows:

S. 1326

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. ASSISTANT SECRETARY OF COMMERCE FOR MANUFACTURING.

(a) ESTABLISHMENT.—There is in the Department of Commerce the position of Assistant Secretary of Commerce for Manufacturing. The Assistant Secretary shall be appointed by the President by and with the advice and consent of the Senate.

(b) DUTIES.—The Assistant Secretary of Commerce for Manufacturing shall—

(1) represent and advocate for the interests of the manufacturing sector;

(2) aid in the development of policies that promote the expansion of the manufacturing sector;

(3) review policies that may adversely impact the manufacturing sector; and

(4) perform such other duties as the Secretary of Commerce shall prescribe.

(c) REPORTING REQUIREMENTS.—The Assistant Secretary of Commerce for Manufacturing shall submit to Congress an annual report that contains the following:

(1) An overview of the state of the manufacturing sector in the United States.

(2) A forecast of the future state of the manufacturing sector in the United States.

(3) An analysis of current and significant laws, regulations, and policies that adversely impact the manufacturing sector in the United States.

(d) COMPENSATION.—Section 5314 of title 5, United States Code, relating to Level IV of the Executive Schedule, is amended by inserting before "and Assistant" in the item relating to the Assistant Secretaries of Commerce the following: "Assistant Secretary of Commerce for Manufacturing,".

By Mr. CORZINE:

S. 1327. A bill to reduce unsolicited commercial electronic mail and to protect children from sexually oriented advertisements; to the Committee on Commerce, Science, and Transportation.

Mr. CORZINE. Mr. President, today I am introducing legislation, the Restrict and Eliminate the Delivery of Unsolicited Commercial Electronic Mail, REDUCE, Spam Act, to curb the influx of unwanted junk e-mail, or "spam," that is clogging our inboxes and wasting the time and money of American consumers and businesses.

The flood of spam is growing so fast that it will soon account for more than half of all e-mail sent in the United States. Spam already accounts for nearly 40 percent of e-mail traffic, and costs U.S. businesses $10 billion annually in lost productivity and additional equipment, software and manpower costs necessary to manage this burden. Microsoft Inc. estimates that more than 80 percent of the more than 2.5 billion e-mail messages sent each day to Hotmail users are spam. And data suggests that the problem is only growing.

The problem of spam goes well beyond inconvenience and cost. The Federal Trade Commission examined a random sample of 1000 spam messages and, in a report issued on April 30, 2003, found staggering evidence of fraud. According to the report, 33 percent of the messages sampled contained false routing information; 22 percent contained false information in the subject line; 40 percent contained false statements in the text; and a full 66 percent contained false information of some sort. Most alarmingly, in the case of spam touting business or investment opportunities, 96 percent contained some sort of fraudulent information.

In addition, pornographic spam is a growing problem for parents trying to shield their children from such images. The FTC report found that 17 percent of spam advertising pornographic websites included adult images in the body of the message. This is not acceptable when our children are using email more and more each day.

Unfortunately, it is very difficult to track down those who send spam. Often, spammers use multiple e-mail addresses or disguise routing information to avoid being identified. Finding spammers can take not just real expertise, but persistence, time, energy and commitment.

To attack the problem of spam, my proposal adopts a two-prong approach championed by the leading thinker about cyberlaw, Professor Lawrence Lessig of Stanford Law School. Congresswoman ZOE LOFGREN also has introduced similar legislation in the House of Representatives. The approach is simple: first, anyone sending bulk unsolicited commercial e-mail would have to include on each e-mail a simple prefix—either ADV: or ADV:ADLT. Second, anyone who finds a spam-source who has failed to properly label unsolicited commercial e-mail would be eligible for a monetary reward from the FTC.

The first part of this proposal would enable Internet Service Providers, ISPs, employers and individual users to filter spam from business and personal email. This would give people the ability to tell their Internet service provider to block ADV e-mail, or they could automatically filter such e-mail into a spam folder on their own computer. This approach would enable far more effective filtering than currently possible.

The second part of my proposal would require the FTC to pay a bounty to anyone who tracks down a spammer who has failed properly to label unsolicited commercial e-mail. The proposal would invite anyone across the world who uses the Internet to hunt down these law-violating spammers. The FTC would then fine them and pay a portion of that fine as a reward to the bounty hunter who found them. The FTC could use the remainder of the fine to track down and prosecute other spammers.

Creating incentives for private individuals to help track down spammers is likely to substantially strengthen the enforcement of anti-spam laws. And with proper enforcement, spammers would soon learn that neglecting to label spam does not pay. In the end, that will mean that more spammers will label their spam or give up and stop spamming altogether. Either way, we will have fixed, or at least started to fix, the problem.

Professor Lessig is so convinced that this approach will substantially reduce spam that he has pledged to resign from his job at Stanford if it does not. While I will not hold him to that warranty, I do share his enthusiasm about this innovative approach, which is likely to be much more effective than relying exclusively on government investigators to identify spammers.

Having said that, I recognize that any domestic anti-spam legislation potentially is subject to evasion by spammers who relocate overseas in order to continue sending spam. To respond to that possibility, my bill also orders the Administration to study the possibility of an international agreement to reduce spam. This is an issue that affects us globally, and, in my view, we should consider a coordinated response.

In addition to these primary provisions, my bill would require marketers to establish a valid return e-mail address to which an e-mail recipient can write to "opt-out" of receiving further e-mails, and would prohibit marketers from sending any further e-mails after a person opts-out. The bill also would prohibit spam with false or misleading routing information or deceptive subject headings, and would authorize the Federal Trade Commission to collect civil fines against marketers who violate these requirements. Furthermore, my proposal would give Internet Service Providers the right to bring civil actions against marketers who violate these requirements and disrupt their networks, and, finally, the proposal would establish criminal penalties for fraudulent spam.

I know that the Commerce Committee recently ordered reported legislation to deal with the problem of spam, and I am hopeful that bill will come before the full Senate before long. When it does, it is my intention to work with my colleagues to see if some of the concepts in the REDUCE Spam Act, such as the establishment of individual rewards for bounty hunters, and a report on a possible international agreement on spam, can be incorporated into the broader package, to ensure that any legislation sent to the President will actually be effective in reducing spam.

I ask unanimous consent that the text of the legislation be printed in the

RECORD at this point, along with a related article by Professor Lawrence Lessig.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

S. 1327

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled.

SECTION 1. SHORT TITLE.

This Act may be cited as the "Restrict and Eliminate the Delivery of Unsolicited Commercial Electronic Mail or Spam Act of 2003" or the "REDUCE Spam Act of 2003".

SEC. 2. DEFINITIONS.

In this Act:

(1) COMMERCIAL ELECTRONIC MAIL MESSAGE.—

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

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

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

(3) ELECTRONIC MAIL ADDRESS.—

(A) IN GENERAL.—The term "electronic mail address" means a destination (commonly expressed as a string of characters) to which an electronic mail message 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").

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

(5) HEADER INFORMATION.—The term "header information" means the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address.

(6) 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, either directly or through an agent, but shall not include actions that constitute routine conveyance of such message by a provider of Internet access service. For purposes of this Act, more than 1 person may be considered to have initiated the same commercial electronic mail message.

(7) 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)).

(8) 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)).

(9) PRE-EXISTING BUSINESS RELATIONSHIP.—

(A) IN GENERAL.—The term "pre-existing business relationship", when used with respect to a commercial electronic mail message, means that either—

(i) within the 5-year period ending upon receipt of a commercial electronic mail message, there has been a business transaction between the sender and the recipient, including a transaction involving the provision, free of charge, of information, goods, or services requested by the recipient and the recipient was, at the time of such transaction or thereafter, provided a clear and conspicuous notice of an opportunity not to receive further commercial electronic mail messages from the sender and has not exercised such opportunity; or

(ii) the recipient has given the sender permission to initiate commercial electronic mail messages to the electronic mail address of the recipient and has not subsequently revoked such permission.

(B) APPLICABILITY.—If a sender operates through separate lines of business or divisions and holds itself out to the recipient as that particular line of business or division, then such line of business or division shall be treated as the sender for purposes of subparagraph (A).

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

(11) SENDER.—The term "sender", when used with respect to a commercial electronic mail message, means the person who initiates such message. The term "sender" does not include a provider of Internet access service whose role with respect to electronic mail messages is limited to handling, transmitting, retransmitting, or relaying such messages.

(12) UNSOLICITED COMMERCIAL ELECTRONIC MAIL MESSAGE.—The term "unsolicited commercial electronic mail message" means any commercial electronic mail message that—

(A) is not a transactional or relationship message; and

(B) is sent to a recipient without the recipient's prior affirmative or implied consent.

SEC. 3. COMMERCIAL ELECTRONIC MAIL CONTAINING FRAUDULENT HEADER OR ROUTING INFORMATION.

(a) IN GENERAL.—Chapter 63 of title 18, United States Code, is amended by adding at the end the following:

"§ 1351. Unsolicited commercial electronic mail containing fraudulent header information

"(a) Any person who initiates the transmission of any unsolicited commercial electronic mail message, with knowledge and intent that the message contains or is accompanied by header information that is false or materially misleading, shall be fined or imprisoned for not more than 1 year, or both, under this title.

"(b) For purposes of this section, the terms 'unsolicited commercial electronic mail message' and 'header information' have the meanings given such terms in section 2 of the REDUCE Spam Act of 2003.".

(b) CONFORMING AMENDMENT.—The chapter analysis at the beginning of chapter 63 of title 18, United States Code, is amended by adding at the end the following:

"1351. Unsolicited commercial electronic mail.".

SEC. 4. REQUIREMENTS FOR UNSOLICITED COMMERCIAL ELECTRONIC MAIL.

(a) SUBJECT LINE REQUIREMENTS.—It shall be unlawful for any person to initiate the transmission of an unsolicited commercial electronic mail message to an electronic mail address within the United States, unless the subject line includes—

(1) except in the case of an unsolicited commercial electronic mail message described in paragraph (2)—

(A) an identification that complies with the standards adopted by the Internet Engineering Task Force for identification of unsolicited commercial electronic mail messages; or

(B) in the case of the absence of such standards, "ADV:" as the first four characters; or

(2) in the case of an unsolicited commercial electronic mail message that contains material that may only be viewed, purchased, rented, leased, or held in possession by an individual 18 years of age and older—

(A) an identification that complies with the standards adopted by the Internet Engineering Task Force for identification of adult-oriented unsolicited commercial electronic mail messages; or

(B) in the case of the absence of such standards, "ADV:ADLT" as the first eight characters.

(b) RETURN ADDRESS REQUIREMENTS.—

(1) ESTABLISHMENT.—It shall be unlawful for any person to initiate the transmission of an unsolicited commercial electronic mail message to an electronic mail address within the United States, unless the sender establishes a valid sender-operated return electronic mail address where the recipient may notify the sender not to send any further commercial electronic mail messages.

(2) INCLUDED STATEMENT.—All unsolicited commercial electronic mail messages subject to this subsection shall include a statement informing the recipient of the valid return electronic mail address referred to in paragraph (1).

(3) PROHIBITION OF SENDING AFTER OBJECTION.—Upon notification or confirmation by a recipient of the recipient's request not to receive any further unsolicited commercial electronic mail messages, it shall be unlawful for a person, or anyone acting on that person's behalf, to send any unsolicited commercial electronic mail message to that recipient. 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.

(c) HEADER AND SUBJECT HEADING REQUIREMENTS.—

(1) FALSE OR MISLEADING HEADER INFORMATION.—It shall be unlawful for any person to initiate the transmission of an unsolicited commercial electronic mail message that such person knows, or reasonably should know, contains or is accompanied by header information that is false or materially misleading.

(2) DECEPTIVE SUBJECT HEADINGS.—It shall be unlawful for any person to initiate the transmission of an unsolicited commercial electronic mail message with a subject heading that such person knows, or reasonably should know, is likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message.

(d) AFFIRMATIVE DEFENSE.—A person who violates subsection (a) or (b) shall not be liable if—

(1)(A) the person has established and implemented, with due care, reasonable practices and procedures to effectively prevent such violations; and

(B) the violation occurred despite good faith efforts to maintain compliance with such practices and procedures; or

(2) within the 2-day period ending upon the initiation of the transmission of the unsolicited commercial electronic mail message in violation of subsection (a) or (b), such person initiated the transmission of such message, or one substantially similar to it, to less than 1,000 electronic mail addresses.

SEC. 5. ENFORCEMENT.

(a) IN GENERAL.—Section 4 shall be enforced by the Commission under the FTC

Act. For purposes of such Commission enforcement, a violation of this Act shall be treated as a violation of a rule under section 18 (15 U.S.C. 57a) of the FTC Act prohibiting an unfair or deceptive act or practice.

(b) RULEMAKING.—Not later than 30 days after the date of enactment of this Act, the Commission shall institute a rulemaking proceeding concerning enforcement of this Act. The rules adopted by the Commission shall prevent violations of section 4 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, except that the rules shall also include—

(1) procedures to minimize the burden of submitting a complaint to the Commission concerning a violation of section 4, including procedures to allow the electronic submission of complaints to the Commission;

(2) civil penalties for violations of section 4 in an amount sufficient to effectively deter future violations, a description of the type of evidence needed to collect such penalties, and procedures to collect such penalties if the Commission determines that a violation of section 4 has occurred;

(3) procedures for the Commission to grant a reward of not less than 20 percent of the total civil penalty collected to the first person that—

(A) identifies the person in violation of section 4; and

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

(4) a provision that enables the Commission to keep the remainder of the civil penalty collected and use the funds toward the prosecution of further claims, including for necessary staff or resources; and

(5) civil penalties for knowingly submitting a false complaint to the Commission.

(c) REGULATIONS.—Not later than 180 days after the date of enactment of this Act, the Commission shall conclude the rulemaking proceeding initiated under subsection (b) and shall prescribe implementing regulations.

SEC. 6. PRIVATE RIGHT OF ACTION.

(a) ACTION AUTHORIZED.—A recipient of an unsolicited commercial electronic mail message, or a provider of Internet access service, adversely affected by a violation of section 4 may bring a civil action in any district court of the United States with jurisdiction over the defendant to—

(1) enjoin further violation by the defendant; or

(2) recover damages in an amount equal to—

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

(B) at the discretion of the court, the amount determined under subsection (b).

(b) STATUTORY DAMAGES.—

(1) IN GENERAL.—For purposes of subsection (a)(2)(B), the amount determined under this subsection is the amount calculated by multiplying the number of willful, knowing, or negligent violations by an amount, in the discretion of the court, of up to $10.

(2) PER-VIOLATION PENALTY.—In determining the per-violation penalty under this subsection, the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, the extent of economic gain resulting from the violation, and such other matters as justice may require.

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

SEC. 7. INTERNET ACCESS SERVICE PROVIDERS.

Nothing in this Act shall be construed—

(1) to enlarge or diminish the application of chapter 121 of title 18, relating to when a provider of Internet access service may disclose customer communications or records;

(2) to require a provider of Internet access service to block, transmit, route, relay, handle, or store certain types of electronic mail messages;

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

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

SEC. 8. EFFECT ON OTHER LAWS.

Nothing in this Act shall be construed to impair the enforcement of section 223 or 231 of the Communications Act of 1934 (47 U.S.C. 223 or 231), 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.

SEC. 9. FTC STUDY.

Not later than 24 months after the date of enactment of this Act, the Commission, in consultation with appropriate agencies, shall 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 Congress to modify such provisions.

SEC. 10. STUDY OF POSSIBLE INTERNATIONAL AGREEMENT.

Not later than 6 months after the date of enactment of this Act, the President shall—

(1) conduct a study in consultation with the Internet Engineering Task Force on the possibility of an international agreement to reduce spam; and

(2) issue a report to Congress setting forth the findings of the study required by paragraph (1).

SEC. 11. EFFECTIVE DATE.

The provisions of this Act shall take effect 180 days after the date of enactment of this Act, except that subsections (b) and (c) of section 5 shall take effect upon the date of enactment of this Act.

[From the Philadelphia Inquirer, May 4, 2003]

HOW TO UNSPAM THE INTERNET

(By Lawrence Lessig)

The Internet is choking on spam. Billions of unsolicited commercial messages—constituting almost 50 percent of all e-mail traffic—fill the in-boxes of increasingly impatient Internet users. These messages offer to sell everything from human growth hormones to pornography. And increasingly the offers to sell pornography are themselves pornographic.

So far, Congress has done nothing about this burden on the Internet. Many states have passed laws that have cried. Virginia just passed the most extreme of these laws, making it a felony to send spam with a fraudulent return address. Other states are considering the same.

Yet all of these regulations suffer from a similar flaw: Spamsters know the laws will never be enforced. The cost of bringing a lawsuit is extraordinarily high. Most of us have better things to do than sue spamsters. Thus, despite a patchwork of regulation that in theory should be restricting spam, the practice of spam continues to increase at an astonishing rate.

But last week, U.S. Rep. Zoe Lofgren (D., Calif.) introduced a bill that, if properly implemented by the Federal Trade Commission, would actually work. I am so confident she is right that I've offered to resign my job if her proposal does not significantly reduce the burden of spam.

The Restrict and Eliminate Delivery of Unsolicited Commercial E-mail (REDUCE) Spam Act has two important parts. First, anyone sending bulk unsolicited commercial e-mail must include on each e-mail a simple tag—either ADV: or ADV:ADLT. Second, anyone who finds a spamster who fails properly to label unsolicited commercial e-mail will be paid a bounty by the FTC.

The first part of the proposal would enable simple filters to block unwanted spam. Users could tell their Internet service provider to block ADV e-mail, or they could automatically filter such e-mail into a spam folder on their own computer. These simple filters would replace the extraordinarily sophisticated filters companies have been developing to identify and block spam.

These complex filters, though ingenious, are necessarily one step behind. Spamsters will always find a way to trick them. The filters will be changed to respond, but the spamsters will in turn change their spam to find a way around the filters. Thus the filters will never block all spam, but they will always block a certain number of messages that are not spam.

But part one of the Lofgren legislation would never work if it weren't for part two: A spamster bounty. Lofgren's proposal would require the FTC to pay a bounty to anyone who tracks down a spamster who has failed properly to label unsolicited commercial e-mail. This proposal would invite savvy 18-year-olds from across the world to hunt down these law-violating spamsters. The FTC would then fine them, after paying a reward to the bounty hunter who found them.

The bounty would assure that the spam law was enforced. Properly enforced, the law would teach most spamsters that failing to label spam doesn't pay. The spamsters in turn would decide either to label their spam or give up and get a real job. Either way, the burden of spam would be reduced.

No doubt no solution would eliminate 100 percent of spam. Much is foreign; American laws would not easily reach those spamsters. But the question lawmakers should ask is what is the smallest, least burdensome regulation that would have the most significant effect. If Lofgren's proposal were passed, the vast majority of spamsters would have to change their ways. Technologists could then target their filters on the spamsters that remain.

What about free speech? Don't spamsters have First Amendments rights?

Of course they do. And many of the laws proposed right now go too far in censoring speech. Threatening a felony for a bad return address, as the Virginia law does, is a dangerous precedent. Laws that ban spam altogether are much worse.

But Lofgren's proposal simply requires a proper label so consumers can choose whether they want to receive the speech or not. And most important, by reducing the clutter of unsolicited and unwanted spam, the law would improve the opportunity for other speech—including political speech—to get through.

More fundamentally, free speech is threatened just as much by bad filters as by bad laws. A well-crafted law—narrow in its scope, and moderate in its regulation—can in turn eliminate the demand for bad filters. Lofgren's proposal would have just this effect. Congress should act to follow Lofgren's lead. In Internet time, not Washington time.

By Mr. HATCH (for himself and Mrs. CLINTON):

DOCUMENT NO. 7