

or has engaged in any falsified spamming technique prohibited by Section 5(a)(1) or 18 U.S.C. 1037, the Act is intended to be read so that such a procurer meets the standard of "conscious avoidance of actual knowledge" of violations of the Act by an initiator unless the procurer and takes reasonable steps to prevent such violations by the initiator.

Actual knowledge or conscious avoidance of actual knowledge could be evidenced, for example, by information obtained by the procurer directly from an initiator, or via a complaint, warning or cease and desist communication received from a recipient, Internet access service, or law enforcement alerting the procurer that an initiator to whom the procurer is providing consideration is violating the law. Conscious avoidance of actual knowledge could also be evidenced, for example, by: (1) Doing little or nothing to determine whether suspect initiators who are marketing partners, resellers, affiliates, agents or contractors of the procurer are violating or have violated Federal or State law; (2) failing to follow the procurer's stated policies or procedures prohibiting illegal e-mail advertising methods by initiators who are marketing partners, resellers, affiliates, agents or contractors; (3) repeatedly allowing initiators who are engaged in illegal e-mail advertising methods to provide false information or to fail to identify themselves when they sign up to conduct e-mail advertising for the procurer's products or services; (4) repeatedly paying initiators whom the procurer has terminated for violating the procurer's e-mail policies prohibiting illegal spamming methods; or (5) allowing initiators who have been terminated for violating the procurer's policies prohibiting illegal e-mail activities repeatedly to sign up for new accounts. The above is not an exhaustive list of ways in which the requisite state of mind can be evidenced.

Subparagraphs (f) and (g) allow enforcement actions for violations of certain parts of Section 5 to be brought by States and ISPs only for a "pattern or practice" of violations. The Act regulates a wide variety of commercial e-mail practices, some of which are deemed more deplorable than others and subject to higher penalties.

Such action may seek to enjoin further violations by defendants, or collect certain limited monetary damages. It is our intention that these cases be based on bona fide violations and not used as tools for anti-competitive behavior among competitors. Additionally, we intend that Internet access service providers provide actual Internet access service to customers.

Statutory damages for Internet service providers are at a lower level than those provided to federal and state regulators.

Section 8 provides for the effect of the legislation on other law.

Section (b) provides for preemption of state laws that expressly regulate the use of e-mail to send commercial messages, including laws that regulate the form or manner of sending commercial e-mail (e.g. labeling requirements). It does not preempt statutes dealing with fraud, falsity, or deception in any portion of a commercial e-mail message or attachment thereto. Thus, State opt-in spam laws, such California S.B. 186 enacted in the fall of 2003, state opt-out spam laws, and state ADV labeling requirements for commercial e-mail would be entirely preempted, except to the

limited extent that those laws also prohibited use of falsification techniques or deception such as those prohibited in 18 U.S.C. 1037, Section 5(a)(1) and Section 5(a)(2) of this Act. Similarly, State anti-spam laws, such as Virginia's, that expressly regulate or criminalize e-mail falsification techniques would not be preempted. In addition, Section 8(b) is not intended to preempt general purpose State deceptive trade practice laws, or State common law rules, such as State trespass to chattels theories, that have been used in anti-spam litigation. Nor does Section 8(b) preempt State laws relating to acts of fraud or computer crime. However, to the extent any State or local law regulates the manner of sending commercial e-mail, the mere titling of the law as an "anti-fraud statute" or the combination of commercial e-mail regulation provisions with actual falsification or computer crime provisions in the same statute is not sufficient to avoid preemption of those regulatory provisions by this Act.

Section 9 provides the FTC with authority to establish a do not e-mail registry.

The provision requires the FTC to set forth a plan and timetable for establishing a national do not e-mail registry. The FTC is required to report to the Congress on any practical, technical, security, privacy, enforceability or other concerns the FTC may have with such a registry.

We expect that the FTC will proceed with due care in this important inquiry. In particular, the FTC should take care not to inadvertently adopt a do not e-mail registry that would facilitate the availability of working e-mail addresses to persons who might use them in violation of this Act.

Section 14 requires the FCC to promulgate rules to prevent the sending of unsolicited e-mail messages to wireless customers, without the express consent of such customers.

S. 877—CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING ACT OF 2003—CAN-SPAM ACT OF 2003 (PL 108-187)

**HON. W.J. (BILLY) TAUZIN**

OF LOUISIANA

IN THE HOUSE OF REPRESENTATIVES

Wednesday, January 28, 2004

Mr. TAUZIN. Mr. Speaker, this statement represents my views as well as the views of the Ranking Member of the Committee on Energy and Commerce, JOHN DINGELL, on S. 877, the CAN-SPAM Act of 2003 ("the Act"). The House passed S. 877 by unanimous consent on December 8, 2003, and the President signed S. 877 into law on December 16th 2003 (Public Law 108-187). These views are in addition to those included in the November 21, 2003 and December 16, 2003, floor debate on S. 877.

The purpose of the CAN-SPAM Act of 2003 is to prohibit certain predatory and abusive practices used to send commercial e-mail, provide consumers with the ability to more easily identify and opt-out of receiving other unwanted commercial e-mail, and to give such opt-outs the force of law. The legislation provides enforcement tools to the Federal Trade Commission (FTC), the Department of Justice (DOJ), other Federal regulators, States' Attor-

neys General and bona fide Internet service providers (ISPs) to enforce compliance with the Act.

The Act's scope provides extensive jurisdiction over commercial e-mail by, among other things, cross-referencing definitions of terms such as "protected computer" as that term is used in Section 1037(e) of Title 18, United States Code. This jurisdiction may be interpreted to extend extraterritorially. It is the intent of the Act to broadly assert jurisdiction over commercial e-mails—from any source—that are sent to U.S. recipients or that use protected computers in the U.S. to affect any of the deceptive spamming activities prohibited in Section 1037 of Title 18 or Section 5(a)(1) of the Act's civil provisions, as well as jurisdiction over computers and computer servers engaged in communication with the United States which are used to send such commercial e-mails that otherwise cause harm to commerce in the United States. However, the managers also recognize that because of the nature of the Internet, commercial e-mail which is in no way falsified may transit the United States as a matter of routine conveyance without the knowledge of the initiator or sender, without being received by any U.S. consumers and with minimal impact here. For example, a travel agency located in Spain using computers that are sometimes in communication with the United States might send unfalsified commercial e-mail promoting travel specials exclusively to consumers in Chile but those e-mails would be routed as a matter of course through computer servers located in California without the knowledge of the initiator or sender. The Act is not intended to regulate the contents of such legitimate commercial e-mail messages (by, for instance, imposing the Act's required inclusions and opt-out regime) merely because they transit the United States or are sent from computers in communication with the United States, provided such commercial e-mails are not falsified in a manner prohibited by Section 1037 of Title 18, or Section 5(a)(1) or directed to or received by U.S. consumers and do not otherwise cause harm here.

Section 1 of the legislation sets forth the short title, the CAN-SPAM Act of 2003.

Section 2 of the legislation sets forth various Congressional findings and determinations. Such findings and determinations are in addition to those in this statement.

Section 3 sets forth definitions.

The term "Commercial electronic mail message" is defined as any e-mail message, the primary purpose of which is commercial advertisement or promotion of a commercial product or service. The definition of commercial electronic mail message does not include transactional e-mail. The purpose of this provision and its relationship to the definition of "transactional or relationship message" is to exclude from most of the requirements of the legislation, e-mail messages that are pursuant to existing transactional relationships between a consumer and an e-mail sender.

The term "Electronic mail message" is intended to capture e-mail messages sent to a unique electronic mail address as that term is commonly understood and should be read to include messages sent to a unique electronic mail address where the reference to the Internet domain or "domain part" in the message is implicit and does not appear or is not displayed explicitly. This is not intended to expand or contract the commonly understood

concept of "Electronic mail message" and "Electronic mail address" but to ensure the bill covers those e-mail messages where either the domain part is implicit or is added upon transmission or delivery of the message to a recipient by the owner of the Internet domain to facilitate delivery of the message.

Section 4 sets forth civil and criminal penalties for fraudulent, abusive and predatory commercial e-mail.

The section provides that intentionally sending multiple commercial e-mail messages from a protected computer without authorization is subject to the penalties set forth in subsection (b) of section 4. The purpose of this provision is to prevent fraudulent use of third party's computer for purposes of sending commercial e-mail.

The section also provides that materially falsifying header information in multiple commercial e-mails is subject to the penalties set forth in subsection (b) of section 4. The purpose of this provision is to prevent fraudulent practices that disguise the route or source of a commercial e-mail message.

The section also provides that using information that materially falsifies the identity of the actual registrant for five or more e-mail accounts or online user accounts, or two or more domain names, and intentionally sending commercial e-mail messages from any combination of such addresses or accounts is a violation of this Act and subject to the penalties set forth in subparagraph (b) of section 4. The term "online user accounts" is meant to include registration for an account on a website that facilitates sending of e-mail messages to other users of such website. The purpose of this provision is to prevent the fraudulent establishment of e-mail accounts, online user accounts, web addresses or domain names from or through which unwanted commercial e-mail messages are intentionally sent or routed.

The section also provides that one who falsely represents one's self to be the registrant or bona fide successor in interest to the registrant of five or more Internet protocol addresses and intentionally sends multiple commercial e-mails from such addresses is subject to the penalties set forth in subsection (b) of section 4.

Subsection (b) of section 4 sets forth criminal penalties under the legislation. An offense as defined in section 4 is punishable by a fine or imprisonment of not more than five years or both if the offense is committed in furtherance of a felony (other than one defined in this Act), or the defendant has previously been convicted of a criminal offense under this Act or under the laws of any State, for conduct involving the sending of multiple unlawful commercial e-mail messages or unauthorized access to a computer system. Other violations under section (b) are punishable by a fine or imprisonment of not more than three years, or both.

Section 4 (in newly created 18 U.S.C. 1037(d)(2)) and Section 5(a)(6) contain definitions of "materially" that apply to certain falsification violations of the Act's criminal and civil provisions. The phrase "identify, locate, or respond" as used in this definition is intended to be interpreted broadly to encompass all methods of technical falsification that impede the ability of the recipient, an ISP, the FTC or appropriate Federal regulator, the DOJ, or a State Attorney General either to identify the source of the e-mail or whether the e-mail

comes from an approved or known sender, to locate or bring enforcement action against an initiator of the e-mail, or to respond by taking countermeasures against or transmitting the e-mail message back to the initiator. Materially falsifying may also include, for example, falsifying certificates or similar sender authentication mechanisms used by a recipient or an Internet access service to identify the source of an e-mail message.

Section 5 of the legislation sets up a regulatory regime for sending commercial e-mail messages.

The section prohibits the sending of commercial e-mail messages or transactional or relationship messages with headings that are materially false or materially misleading. The section also prohibits knowingly sending commercial e-mail messages with deceptive subject headings.

The section requires a person sending commercial e-mail messages to conspicuously identify such messages as a solicitation or advertisement and provide to each recipient a conspicuous means of opting-out from receiving subsequent commercial e-mail messages. The term "clear and conspicuous" as it applies to the requirements of Section 5(a) is intended to be consistent with the meaning of that term as set forth in FTC guidance documents (e.g. "Dot-Com Disclosures" available via online publications at <http://www.ftc.gov>). It is intended that a required inclusion can meet the "clear and conspicuous" standard in a number of ways. The Act does not authorize the FTC to require the notice to be placed in a specific location such as the subject line or body of a commercial e-mail. The FTC is required by this Act to conduct a study of required labels in the subject line of commercial e-mail messages but cannot prescribe an inclusion of such label or notices in the subject line without further Congressional action. In addition, the sender of the commercial e-mail message must provide a reply e-mail address or other Internet-based mechanism, such as a clear and conspicuous link to an opt-out form, on a website that will enable recipients to reject further commercial communications within the scope of the opt-out from the sender. In addition, the sender must ensure the return e-mail address or other form of Internet-based communication is capable of receiving opt-outs for not less than 30 days from the transmission of each commercial e-mail message. We intend that senders of commercial e-mail provide a convenient, clear and simple way for consumers to opt-out of commercial e-mail. We also intend that senders of commercial e-mail devote sufficient resources to monitoring and maintaining records of consumer opt-outs so that giving effect to these consumers' opt-outs will be prompt and permanent.

The section expressly provides that senders of commercial e-mail may provide recipients with a menu of options of commercial e-mail messages that the recipient may or may not wish to receive. Such a menu must include the option of receiving no additional commercial e-mail messages. An opt-out menu gives consumers the option to continue to receive a sub-group of defined communications from a sender, if the consumer so desires.

The section provides that senders must give effect to customer opt-outs within ten business days of receiving such opt-outs. This time period is subject to regulatory modification by the FTC as described below. It further provides

that subsequent affirmative consent by a consumer (an opt-in) will allow a sender lawfully to send commercial e-mail to a consumer so consenting. The burden of proving subsequent affirmative consent should be on the sender in any dispute between a sender and a recipient of commercial e-mail.

This provision prohibits the sender, or any other person who knows that the recipient has made an opt-out request, from selling, leasing, exchanging or otherwise transferring or releasing the e-mail address of the recipient other than for purposes of compliance with this Act or any other law.

Subparagraph (5) of section 5(a) sets forth specific required inclusions in commercial e-mail. These include clear and conspicuous identification that the message is an advertisement or a solicitation; a clear and conspicuous notice of the opportunity to opt-out of receipt of subsequent commercial e-mail messages; and a valid physical postal address of the sender.

Subsection (b) of section 5 provides that harvesting e-mail addresses or generating e-mail addresses by means of a dictionary attack constitutes an aggravating factor for illegal transmission of commercial e-mail under subsection (a) of section 5. Use of automated means to generate e-mail addresses, or gathering e-mail addresses is not by itself illegal, unless the commercial e-mail messages sent to the generated or harvested addresses as a result of such activity do not comply with the requirements of subsection (a).

Subpart (2) makes reference to online user accounts. As in section 4, the term online user accounts is meant to include registration for an account on a website that facilitates sending of e-mail to other users of such website or any other protected computer not affiliated with the website.

Subsection (c) of section 5 requires the FTC to conduct a rulemaking on the 10-day period required for e-mail senders to comply with customers' opt-out requests. As technology allows, we hope that that period will be shortened.

Subsection (d) sets forth additional requirements for transmission of commercial e-mail messages containing sexually explicit material. In particular, such e-mail messages must alert recipients in the subject heading of the e-mail that the message contains sexually explicit material. Additionally, the sender must provide a means of opting-out from receipt of such messages in a manner that does not involve viewing sexually explicit images.

My views, as well as those of Ranking Member JOHN DINGELL, regarding Sections six through 16 of the Act are continued in the Statement of JOHN DINGELL submitted contemporaneously with this statement.

#### PERSONAL EXPLANATION

**HON. PATRICK J. TIBERI**

OF OHIO

IN THE HOUSE OF REPRESENTATIVES

*Wednesday, January 28, 2004*

Mr. TIBERI. Mr. Speaker, on January 27, 2004, the flight I was scheduled to travel on from Columbus, OH to Washington D.C. was cancelled due to weather. As a result, I was unable to cast a vote on Rollcalls 6 and 7. Had I been able, I would have voted "yea" on