CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

CDT's Analysis of S. 877
Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003

December 11, 2003

On December 8, 2003, the U.S. House of Representatives passed by unanimous consent an amended version of S. 877, the "CAN-SPAM Act," sponsored by Senators Conrad Burns (R-MT) and Ron Wyden (D-OR). Coming after the Senate's November 25 passage of identical language, the House action sends the legislation to the President, who is expected to sign it.

Section 3: Definitions

The final version of the bill sets rules for commercial email and, unlike earlier versions, makes no distinction between solicited and unsolicited commercial email.

A "commercial electronic mail message" is defined as any electronic mail message whose primary purpose is the commercial advertisement or promotion of a commercial product or service. The definition specifically includes email that promotes content on an Internet website operated for a commercial purpose. However, the reference in a message to a commercial entity or a link to the website of a commercial entity does not, by itself, cause the message to fall under the definition of a commercial electronic email message if the contents indicate a primary purpose other than an advertisement or promotion of a product or service. Sec. 3(2). The Act provides that the Federal Trade Commission (FTC) shall issue regulations defining criteria that would determine "primary purpose."

The definition of commercial electronic email message goes on to state that the term does not include "transactional or relationship messages." Therefore, with only one exception we could identify, none of the bill's provisions apply to transactional or relationship messages. As we note below, this produces some anomalous results.

A "transactional or relationship message" is defined as a message whose primary purpose is to (a) facilitate, complete or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender; (b) provide warranty, product recall or safety information with respect to a commercial product or service used or purchased by the recipient; (c) provide notification concerning a change with respect to an ongoing relationship, such as a subscription, membership, account, or comparable ongoing

commercial relationship; (d) provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved; or (e) deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender. Sec. 3(17). The FTC may expand or contract the definition of transactional or relationship messages "to the extent that such modification is necessary to accommodate changes in electronic mail technology or practices" and accomplish the purposes of the Act. Sec. 3(17)(B).

Section 4: Criminal provisions

Section 4 amends Title 18, the criminal law title of the United State Code, by adding a new Section 1037, "Fraud and related activity in connection with electronic mail." It defines five **criminal violations**:

1. Accessing a protected computer (i.e., any computer connected to the Internet) without authorization and intentionally sending multiple commercial email messages from or through such computer. "Multiple" means more than 100 in a 24-hour period, more than 1000 a month, or more than 10,000 a year.
2. Using a protected computer to relay or re-transmit multiple commercial email messages, with the intent to deceive or mislead recipients, or any Internet access service, as to their origin.
3. Materially falsifying header information in multiple commercial email messages and intentionally initiating their transmission.
4. Registering, using information that materially falsifies the identity of the actual registrant, for 5 or more email accounts or online user accounts or 2 or more domain names and intentionally initiating the transmission of multiple commercial email messages from any combination of such accounts or domain names.
5. Falsely representing oneself to be the registrant or legitimate successor in interest to the registrant of 5 or more Internet addresses and intentionally initiating the transmission of multiple commercial electronic mail messages from those addresses.

Subsection (b) of the new section 1037 provides for criminal penalties, ranging from five years to less than one. Subsection (c) requires the forfeiture of proceeds obtained from the offense and equipment used to commit the offense.

Header information is defined as "the source, destination and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." Sec. 3(8).

Under the criminal provision's **definition of "materially**," header information or registration information is *materially* falsified if it is altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service

processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message. 18 U.S.C. 1037(d)(2), as added by sec. 4(a) of the bill. This definition of material falsification only applies to those who send multiple commercial emails; the reference to registration information only applies to those who register for 5 or more email accounts or 2 or more domain names with false identifying information and use them to send multiple commercial messages. The bill does not prohibit the use of pseudonymous addresses, even for commercial purposes. The exclusion of "transactional and relationship messages" from the definition of commercial email means that the bill does not apply to email sent by sellers on, for example, eBay, where they are facilitating or completing transactions that began with a bid in response to website posting. However, the interplay between the definition of "header information" and the definition of "materially" is not very clear. But it does seem fairly clear that non-spoofed pseudonymous header information is not "materially falsified" under the third paragraph of the criminal provision.

Also, the bill nowhere says that senders of commercial email must identify themselves by personal name – it allows trade names. It is a little unclear, however, whether the bill could prohibit use of non-spoofed email addresses that a user can obtain without being asked to identify oneself. (That is, does one "conceal" registration information if one is not asked to provide it?) Given the importance and value of legitimately obtained, non-spoofed pseudonymous and anonymous email addresses, we believe that it would be unreasonable to interpret the bill as prohibiting their use in otherwise truthful commercial transactions. As this is a criminal provision, some guidance from the Justice Department would be very helpful. Note, also, that section 5 of the bill requires all commercial email to include a valid physical address of the sender.

Section 5: Civil provisions – false or misleading header information; deceptive subject lines; opt-out, required disclosures

Sec. 5(a) sets forth rules for all commercial email:

1. It prohibits **false or misleading header information**. Sec. 5(a)(1) makes it unlawful to initiate the transmission to a protected computer of a commercial email message that contains or is accompanied by materially false or materially misleading header information.

   For purposes of section 5, "materially misleading" header information includes:

   - Header information that its technically accurate but includes an originating email address, domain name, or Internet protocol address the access to which for purposes of initiating the message was obtained by false or fraudulent pretenses or representations;

- Header information attached to a message that fails to identify a protected computer used to initiate the message because the sender knowingly uses another protected computer to relay or retransmit the message to disguise its origin.

A "from" line that accurately identifies any person who sent the message is **not** considered materially false or misleading.

Section 5(a)(6) defines "materially," when used with respect to false or misleading header information, to include the alteration or concealment of header information in a manner that would impair the ability of a person alleging a violation of the statute or a law enforcement agency to identify, locate or respond to the person who initiated the message or to investigate the alleged violation.

Unlike most of the rest of the bill, the prohibition against false or misleading header information also applies to transactional or relationship messages.

2. Sec. 5(a)(2) prohibits **deceptive subject headings** on commercial email. The provision on deceptive subject headings, like most of the provisions of the bill, does not apply to transactional and relationship messages.

3. **Opt-out:** Sec. 5(a)(3) requires that commercial email include a functioning return email address or other Internet-based mechanism, clearly and conspicuously displayed, so that a recipient can submit a reply requesting not to receive future commercial email messages. That email address must remain capable of receiving such opt-out messages for at least 30 days after transmission of the original message.

   Senders of commercial electronic mail may comply by providing the recipient with a list or menu from which he may choose the specific types of messages he does or does not want to receive from the sender, so long as the list or menu includes the option of not receiving *any* unsolicited commercial electronic mail. Sec. 5(a)(3)(B).

4. **If the recipient of an email opts not to receive** commercial email from a sender, then it is unlawful (a) for the sender, more than 10 business days after receipt of the opt-out request, to send the recipient any commercial email message that falls within the scope of the request; (b) for a person acting on behalf of the sender to initiate the transmission or assist in initiating the transmission of a commercial email that such person knows falls within the scope of the opt-out request; or (c) for the sender to sell or otherwise disclose the email address of the recipient to a third party. Sec. 5(a)(4)(A).

The prohibition against sending commercial email after receipt of the opt-out does not apply if the recipient affirmatively consents to receiving commercial message subsequent to exercising the opt-out. Sec. 5(a)(4)(B).

It is implicit in the foregoing, but just to be clear: The bill does not prohibit unsolicited email – it requires every commercial email, solicited or unsolicited, to have an opt-out and prohibits sending further commercial messages to those who exercise the opt-out. The opt-out provision does not apply to transactional or relationship messages.

5. **Required disclosures:** Under section 5(a)(5), all commercial email messages must include:

   - **Advertising identification**: clear and conspicuous identification that the message is an advertisement or solicitation. Sec. 5(a)(5)(A)(i).
   - **Notice of opportunity to opt out**: clear and conspicuous notice of the opportunity to decline to receive further commercial email messages from the sender. Sec. 5(a)(5)(A)(ii).
   - **Physical address**: a valid physical postal address of the sender. Sec. 5(a)(5)(A)(iii).

Sec. 5(b) states that it is an **"aggravated" violation** to send a commercial email message in violation of subsection (a) if the sender had actual knowledge or knowledge fairly implied on the basis of objective circumstances that the email address of the recipient was obtained by:

- **address harvesting**, if the website from which the addresses were harvested posted a notice stating that the operator of the site or online service will not make addresses it maintains available to other parties for purposes of initiating electronic email addresses; or

- **dictionary attacks**.

It is also an aggravated violation to

- **use automated means to register for multiple email accounts** or online user accounts from which to transmit a commercial email message that is unlawful under subsection (a); or

- **engage in hijacking** - knowingly relay or retransmit an unsolicited commercial email message that is unlawful under subsection (a) from a computer or computer network that was accessed without authorization.

Section 5(d): Labeling for sexually oriented material

Sec. 105 (e) is a poorly drafted provision intended to require FTC-regulated **marks or notices in the subject heading of any commercial email that contains sexually**

oriented material. The warning must be placed in the subject heading of the email message, in the **form prescribed by the FTC**.

The provision also provides that the matter initially viewable to the recipient when the message is opened must include only --

- any marks or notices as prescribed by the FTC under the provisions of the statute;

- the information otherwise required to be included with all commercial email, identifying the message as an advertisement or solicitation; a clear notice of the ability to opt out, and a valid physical postal address; and

- instructions on how to access, or a mechanism to access, the sexually oriented material.

Within 120 days after enactment of the statute, **the FTC in consultation with the Attorney General must prescribe the marks or notices** to be included in or associated with unsolicited commercial electronic mail that contains sexually oriented material, in order to inform recipients and to facilitate filtering.

Sexually oriented material is defined for purposes of the section as any material that depicts "sexually explicit conduct" as defined in 18 USC 2256 unless the depiction constitutes a small and insignificant part of the message, the remainder of which is not primarily devoted to sexual matters. 18 USC 2256 defines "sexually explicit conduct" as

> "actual or simulated --
> (A) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
> (B) bestiality;
> (C) masturbation;
> (D) sadistic or masochistic abuse; or
> (E) lascivious exhibition of the genitals or pubic area of any person."

Whoever knowingly violates the provision shall be fined under the criminal code or imprisoned for up to 5 years, or both.

CDT expressed its concerns about this provision in a letter to Members of the House Commerce Committee on October 15, 2003. We noted that we opposed mandatory labeling schemes for the Internet. We also objected particularly to the provisions giving the FTC rulemaking authority to dictate standard markings for email. Involving the FTC in setting technical standards for the Internet. is fundamentally inconsistent with the medium's openness and its decentralized architecture based on voluntary standards. We also noted that, as drafted, the provision prohibited sending commercial email that includes anything more than instructions on how to access sexually oriented material, even if the material is lawful. Thus, as drafted, the provision is not merely a labeling

requirement, but a prohibition on including lawful sexually oriented material directly in a commercial email.

Sec. 6: Liability

Section 6(a) is intended to make companies responsible for the email sent on their behalf. It makes it unlawful for a person to promote, or allow promotion, of that person's business in a commercial email message the transmission of which is in violation of section 5(a)(1) if the person

1. knows or should have known that its business was being promoted in the message;
2. received or expected to receive an economic benefit from the promotion; and
3. took no reasonable action to prevent the transmission or to detect the transmission and report it to the FTC.

Section 6(b) states that a person (referred to as the "third party") that provides goods, products, property or services to another person that violates subsection (a) shall not be liable for the violation unless the third party has more than 50 percent ownership in the trade or business of the person that violated subsection (a) of Sec. 6; or has actual knowledge of the promotion of goods or services in a transmission that violates the statute and receives or expects to receive an economic benefit from the promotion.

Sec 7: Enforcement

Under Section 7(a), the **FTC can enforce** the provisions of the statute as if the violation were an unfair or deceptive trade practice proscribed under the FTC Act.

Under Section 7(b), the statute can also be enforced by **other federal agencies** with jurisdiction over specific sectors. For example, the SEC will enforce the statute against investment advisors, and the FDIC against insured banks.

Under Section 7(e), the FTC and the FCC can obtain cease and desist orders or injunctions to enforce compliance with certain sections of the law without alleging or proving the state of mind that would otherwise be required to show a violation of those specific sections.

Under Section 7(f), **states can enforce** the provisions of the statute in a civil action to enjoin further violation or to obtain damages on behalf of residents of the State. The states can also recover statutory damages of up to $250 per illegal message, up to a total of $2,000,000. There are provisions for treble damages and reduction of damages, depending on the willfulness or due care shown by the defendant. It also provides that in successful actions, the court may award states their attorney fees.

Under Section 7(g), **Internet Service Providers (ISPs)** adversely affected by commercial email can bring an action to enjoin further violation or recover damages.

The court may require the defendant to pay the ISP's attorney fees. In cases brought by ISPs, statutory damages range from $25 to $100 per email, up to a total of $1 million. Treble damages are available if the court determines that the defendant violated the Act willfully and knowingly, or the defendant's unlawful activity included one or more of the aggravated violations.

Section 8: Preemption - effect on state law

The CAN SPAM Act **preempts state law** except for any state rule that prohibits falsity or deception in any portion of a commercial message or information attached to the commercial message. It also does not pre-empt states laws not specific to electronic mail, such as trespass, contract, or tort law and state laws related to acts of fraud or computer crime. The law also has no effect on policies of providers of Internet access service.

The statute does not affect enforcement of 47 U.S.C. 223 or 231 (the provisions of COPA as it amends the Communications Act of 1934, 47 U.S.C. 201 et seq.). It is also not to be construed to affect enforcement of chapter 71 (relating to obscenity) or chapter 110 (relating to sexual exploitation of children) of title 18.

The statute is not to be construed to affect the FTC's authority to bring enforcement actions under the FTC Act for materially false or deceptive representations or unfair practices in commercial email messages.

Section 9: Do not mail registry

Within six months of the enactment of the statute, the Federal Trade Commission would be required to provide the Senate Committee on Commerce, Science and Transportation and the House Committee on Energy and Commerce with a report that sets forth a plan and timetable for establishment of a nationwide marketing "Do-Not-Email" registry. The report would discuss any FTC concerns about the registry related to practical and technical implementation, privacy, security, and enforceability. The report would also include a discussion about how the registry would be applied with respect to children with email accounts. The bill also includes an authorization, but not a requirement, to implement such a "Do-Not-Email" registry.

Section 10: Study of effectiveness of the Act

Within 24 months of the enactment of the statute, the FTC, in consultation with the Department of Justice and other appropriate agencies, will be required to submit a report to Congress analyzing the effectiveness and enforcement of the provisions of the statute and the need (if any) for Congress to modify the provisions.

The report must include a discussion of the extent to which technological and marketplace developments affect the effectiveness of the statute; analysis and recommendations concerning how to address commercial email that originates outside of

the United States; and options for protecting consumers, including children, from obscene or pornographic email.

Section 11: Reports on rewards for information about violations and ADV labeling

The Act requires that within 9 months of enactment of the statute the FTC report to the Congress about a system for rewarding those who supply information about violations of the statute including procedures for the FTC to grant a reward to the person who identifies the violator and supplies information that leads to collection of a civil penalty by the Commission.

Section 11 also requires that the FTC to set forth a plan for requiring commercial email to be identifiable through use of an "ADV" or similar label in its subject line. The FTC must report on concerns the FTC might have that would recommend against the plan.

Section 13: FTC Rulemaking

Section 13 authorizes the FTC to promulgate rules to implement the Act.

Section 14: Application to wireless technologies

The Act requires that the Federal Communications Commission, in consultation with the Federal Trade Commission, promulgate rules within 9 months to protect consumers from unwanted mobile service commercial messages. The Act instructs the FCC to (1) provide subscribers to commercial mobile services the ability to avoid receiving mobile service commercial messages unless the subscriber has provided express prior authorization to the sender; (2) allow recipients to decline electronically to receive future mobile service commercial messages from a sender. However, the provision goes on to states in subparagraph (3) that the FCC must take into consideration, in determining whether to subject providers of commercial mobile services to paragraph (1), the business relationship between the wireless service provider and the subscriber.

Section 16: Effective date

The provisions of the Act, other than Section 9 (do-not-email registry), take effect on January 1, 2004.

CDT's Observations

With the exception of the labeling requirements, CDT supported in principle the core provisions of the CAN SPAM Act as appropriate, albeit limited steps in addressing spam. All in all, the bill may have some positive effect in slowing the growth of spam, if not actually reducing it. The bill should help ISPs filter spam and sue spammers. Prohibitions on dictionary attacks and harvesting should also be meaningful. It is noteworthy that the Justice Department was quick to issue a statement supporting the bill – it offers prosecutors new grounds on which to prosecute emailers. We trust that the

FTC and some state Attorneys General will diligently use the enforcement mechanisms, and will be open to consumer complaints.

From a consumer perspective, the opt-out provision is useful with respect to legitimate companies. CDT's study of spam earlier this year, "Why Am I Getting All This Spam?" found that legitimate, "brand-name" companies consistently honor opt-out requests. However, CDT advises users not to exercise an opt-out if they are not sure of the legitimacy of the sender – otherwise, users may just be confirming to an outlaw spammer that their email address is valid.

However, passage of this legislation is only one step in the effort to curtail spam. As discussed in the CDT study, consumer awareness of the online behaviors that spammers exploit and effective use of filtering technologies by users and ISPs remain critical to stemming the flow of spam into users' mailboxes.

Also, as noted above, we are somewhat concerned about how the provisions on falsified or concealed header information may be interpreted, although on balance we think that it would be unreasonable to interpret the statute as prohibiting use of non-spoofed pseudonymous email addresses even for multiple commercial emails, so long as the other disclosure requirements of the bill are met.

CDT is also concerned that the bill lacks what might be the most effective means of enforcement – a narrowly drawn individual right of action. We had recommended as a good model the junk fax law, the Telephone Consumer Protection Act (TCPA). It allows individuals to bring claims in small claims court. Under the TCPA there is no burdensome discovery and there are no class actions. Congress did not include such a provision.

Given the difficulties of enforcing inconsistent state laws on the Internet, CDT supported federal preemption of inconsistent state spam laws. But we did so packaged with a proposed individual private right of action, and with the recognition that the effect of the CAN SPAM Act on the amount and nature of spam is highly uncertain, but almost certain to be incomplete. Congress will have to monitor closely the degree to which the law is effective, and we support the reporting provisions in the bill that will assist Congress in doing so. However, we had also recommended that there should be a mechanism to force Congress to revisit the issue substantively. We felt that the best way to do this would have been with a sunset of the preemption. If the preemption provision were to have sunsetted in three to five years, Congress would have been required to formally confront the question of whether the bill was effective. As it is, if this law does not stem the tide of spam, Congress will still face public pressure to pass more effective provisions or open the issue again to state regulation.

For more information, contact: Paula Bruening, pbruening@cdt.org (202) 637-9800