

**CDT's Analysis of S. 877**  
June 24, 2003

On June 19, the Senate Commerce Committee reported an amended version of S. 877, the "CAN-SPAM Act," sponsored by Senators Conrad Burns (R-MT) and Ron Wyden (D-OR). The bill is one of several proposals to regulate commercial email. CDT has called for a focused, substantive dialogue among key stakeholders to find a balanced solution that would help stem the flood of spam consistent with innovation, free speech and other values. We hope that this analysis of S. 877 contributes to that broader dialogue.

**Definitions**

The bill sets rules for two kinds of email: "commercial electronic mail messages" and "unsolicited commercial electronic mail messages." As often in legislation, the definitions are crucial; in this case, they include substantive policy.

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 product or service. Sec. 3(2).

"Unsolicited commercial electronic mail message" means any commercial email that is not a "transactional or relationship message" and is sent to a recipient without the recipient's prior "affirmative" or "implied" consent. Sec. 3(19).

A "transactional or relationship message" is a message whose primary purpose is to (a) facilitate, complete or confirm a transaction; (b) to provide warranty or safety information with respect to a commercial product or service used or purchased by the recipient; (c) to provide notification concerning a change with respect to an ongoing relationship, such as an subscription, membership, account, or comparable ongoing commercial relationship; (d) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved; or (e) to 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(18).

“Affirmative consent” means that the recipient expressly consented to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient’s own initiative and, if the message is from a third party, the recipient was given clear and conspicuous notice at the time the consent was communicated that the recipient’s email address could be transferred to such other party for the purpose of sending commercial email. (Question: does the first half of this definition allow a box to be checked “yes” when an entity is requesting consent, so that the user must uncheck the box to avoid giving consent?) Sec. 3(1).

“Implied consent” means that within the last 3 years there has been a business transaction between the sender and the recipient (including a transaction involving the free provision of information, goods or services requested by the recipient) and the recipient at the time of such transaction or thereafter in the first email received from the sender was provided clear and conspicuous notice of an opportunity to opt-out of receiving unsolicited email from the sender and has not exercised that opportunity. An email message does not have to relate to the subject of the initial transaction in order to fall under implied consent, although it is clear that implied consent does not cover sales to third parties. Sec. 3(9). (Question: can implied consent be revoked, i.e., can those who fail to opt-out at the time of a transaction or in response to the first email change to opt-out?)

### **Criminal provision - false or misleading header information**

The bill prohibits initiating the transmission of a commercial electronic mail message with knowledge and intent that the message contains or is accompanied by header information that is materially false or materially misleading. Sec. 4.

The criminal provision provides for a fine or imprisonment for not more than 1 year, or both.

The criminal provision also specifically provides that header information that is technically accurate but includes an originating electronic mail address the access to which was obtained by means of false pretenses or representations shall be considered materially misleading.

### **Civil provisions – false or misleading header information; deceptive subject lines**

The bill’s civil enforcement provisions prohibit initiating transmission of commercial electronic mail that contains false or misleading header information. Sec. 5(a)(1).

The bill also prohibits initiating transmission of a commercial email message containing a subject heading that the sender knows would be “likely to mislead” a recipient “about a material fact regarding the contents or subject matter of the message.” Sec. 5(a)(2).

## **Civil provisions – opt-out**

The bill requires commercial email to include a return address or an Internet-based mechanism that the recipient can use to submit a request not to receive future commercial electronic mail messages from the sender at the email address where the message was received. Sec. 5(a)(3).

E-mailers may provide recipients with options or menus that they may use to indicate what types of email they wish to receive, so long as the list or menu includes the option of not receiving *any* unsolicited commercial electronic mail

Transactional or relationship messages do not have to include the option of opting-out. Sec. 5(a)(3)(D).

If the recipient of an email opts not to receive unsolicited commercial email from a sender, then it is unlawful (a) for the sender to send the recipient any more unsolicited messages, more than 10 business days after receipt of the opt-out request, (b) for a person acting on behalf of the sender to initiate the transmission or assist in initiating the transmission of an unsolicited 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).

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

## **Labeling**

All unsolicited commercial email must include clear and conspicuous identification that the message is an advertisement or solicitation. Sec. 5(a)(5)(A).

## **Physical address**

All unsolicited commercial email must include a valid physical postal address of the sender. Sec. 5(a)(5)(C).

## **Aggravated civil violations**

The bill provides for *aggravated violations* in cases of:

- dictionary attacks and the harvesting of email addresses from web sites;
- automated creation of multiple email accounts;
- relaying or retransmission through unauthorized access (hijacking accounts).

## **Compliance**

A person who sends email can defend against allegations of violating the law if he can demonstrate that he has established and implemented, with due care, reasonable practices and procedures to effectively prevent violations and that the violation occurred in spite of good faith efforts to maintain compliance with such practices and procedures. Sec. 5(c).

## **Enforcement**

The law would in general be enforced by the Federal Trade Commission (FTC), but with respect to regulated industries (banks, stockbrokers, air carriers) it would be enforced by the respective federal regulatory bodies for that industry. Sec. 6. States and ISPs could also enforce the law. There would be no private right of action for individuals.

### *Federal Trade Commission*

Violations of the Act would be treated as unfair or deceptive acts or practices under the Federal Trade Commission Act.

### *States*

States could bring a civil action under the Act on behalf of its residents, to enjoin violations of the Act or to obtain actual or statutory damages. The bill provides that, in the case of any successful action, the state shall be awarded attorneys fees.

### *Internet Service Providers*

ISPs may bring a civil action to enjoin violation of the Act or to recover actual or statutory damages. The court *may* award reasonable attorneys fees in a successful suit.

### *Damages*

Statutory damages in cases brought by states and ISPs range from \$25 to \$100 per email, up to a total of \$1 million. For those sent in violation of the civil provisions of the Act, statutory damages are up to \$25 per email. 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.

## **Preemption - effect on state law**

S. 877 would supersede 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 would 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 would have no effect on policies of providers of Internet access service. Sec. 7.

## **Do not mail registry**

The FTC is currently establishing a national telemarketing “Do Not Call” list. S. 877 would require that not more than 6 months implementation of the telemarketing Do Not Call list, the FTC must provide to Congress recommendations for a workable plan and timetable for a nationwide “Do Not Email” list modeled on the Do Not Call, or an explanation of issues that cause the Commission to recommend against creating such a list. Sec. 8.

## **Report on effectiveness of the Act**

Not more than 24 months after the date of enactment of the Act, the FTC, in consultation with the Department of Justice and other appropriate agencies, must report to Congress on the effectiveness of the Act and the whether there may be a need to alter its provisions. Sec. 9.

## **Summary**

- Prohibits false or misleading header information in commercial email --
  - misdemeanor criminal penalties for knowingly and intentionally sending email with materially false or materially misleading header information;
  - civil penalties for any false or misleading header information;
- Prohibits deceptive subject lines in commercial email (civil violation);
- Requires opt-out opportunity in commercial email, except for transactional or relationship messages (civil violation);
- Prohibits unsolicited commercial email to those who have opted-out (civil violation);
- Requires labeling and physical address for unsolicited commercial email (civil violation);
- Prohibits dictionary attacks, harvesting of email, and relaying without authorization (civil violation).

For more information, contact: Paula Bruening, [pbruening@cdt.org](mailto:pbruening@cdt.org), Ari Schwartz [ari@cdt.org](mailto:ari@cdt.org), or Jerry Berman, [jberman@cdt.org](mailto:jberman@cdt.org). (202) 637-9800