Spam Laws: The United States CAN-SPAM Act

Given the problems spam can cause for the individuals who receive it, such as wasted time and effort, being exposed to questionable and sometimes offensive materials, and even exposure to scams and identity theft threats, it should come as no surprise that in 2003 the United States drafted the CAN-SPAM Act in 2003.

CAN-SPAM stands for "Controlling the Assault of Non-Solicited Pornography and Marketing." The act was put into place January 2004 to set out requirements for those sending out commercial e-mails, establish penalties for spammers, and give consumers the right to ask e-mailers to stop spamming them. The law covers e-mail that's primary purpose is to advertise or promote a product, service, or website. Personal e-mails and e-mail updates and advertisements that have been consented to are not covered under this law. Also not covered are "transactional or relationship messages," which are e-mails that pertain to agreed-upon transactions or e-mails that update a customers in an existing business relationship. That is because these types of e-mails are not technically spam - they are a result of previous consent or a business relationship. However, if these types of e-mails contain false or misleading information they are in offense of the CAN-SPAM Act.

The CAN-SPAM Act is enforced by the United States Federal Trade Commission (FTC), and the Department of Justice has authority to enforce its criminal sanctions. Other federal and state agencies can enforce the law in their jurisdictions, and Internet service providers can also sue violators.

Requirements and Prohibitions of the CAN-SPAM Act

The CAN-SPAM Act has five main provisions:

- **False and misleading header information is banned** - This means that an e-mail's "From," "To" and routing information, including the originating domain name and address, must be accurate and identify the sender.

- **Deceptive subject lines are prohibited** - The subject line cannot mislead the receiver of the message to open it under false pretenses, thinking it's something else. The receiver must not be mislead as to the contents or subject matter of the e-mail.

- **Opt-out methods must be provided** - A response mechanism must be provided for the receiver to opt-out of any future commercial messages from the sender. In addition, opt-out requests must be processed for at least 30 days after the initial commercial e-mail was sent, and senders have 10 business days after an opt-out request to stop sending messages to that address. Messages cannot be sent to the opt-out requestor on behalf of the sender by any other entity.

- **Commercial e-mail must be identified as an advertisement and it must include the sender's valid physical postal address** The receiver must be clearly informed that the message is an advertisement or solicitation, he must be told he can opt-out of future mailings, and a valid physical postal address must be included in the message.

- **Receivers must be warned of sexually explicit material** - For any message that contains sexually explicit material, the warning “SEXUALLY-EXPLICIT” must be contained in the subject line.

The FTC is also currently looking into establishing a National Do Not Email Registry that would prohibit senders of commercial messages from targeting anyone who puts themselves on the list.

Penalties for Violation of the CAN-SPAM Act

Violation of the provisions of the CAN-SPAM Act are subject to fines of up to $11,000. Deceptive commercial e-mails are also subject to laws banning false or misleading advertising.
Additional fines are also charged to commercial e-mailers who break the provisions of the CAN-SPAM Act and also:

- "Harvest" e-mail addresses from websites or web services prohibiting the use of their directories for sending unsolicited mail
- Generate e-mail addresses using the "dictionary attack" (combining names, numbers, and/or letters in multiple ways to come up with e-mail addresses)
- Use automated ways to register for multiple accounts to send commercial e-mail
- Relay messages through a computer or network without permission

Imprisonment is possible for commercial e-mailers who:

- Send commercial e-mail through a computer they are not authorized to use for that purpose
- Relay or retransmit multiple messages to deceive recipients about the origin of a message
- Falsify header information
- Register for multiple e-mail accounts or domain names with false identities
- Falsely represent themselves as owners of multiple IP addresses used to send commercial messages

Given the existence of the CAN-SPAM Act, it's important that you report spam in your inbox rather than just deleting it so that the spammers can be prosecuted and fined under the law. If we all do this, it can help reduce spam in the future.

Source: http://www.spamlaws.com/