

The “Controlling The Assault Of Non-Solicited Pornography And Marketing Act Of 2003” (CAN-SPAM Act of 2003)

Michael Siavage

MCKENNA LONG & ALDRIDGE LLP

President Bush has signed into law the first comprehensive nationwide anti-spam law. This article explains the provisions of the “Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003,” also known as the “CAN-SPAM Act of 2003,” and provides strategies for compliance.

Overview Of The CAN-SPAM Act

The CAN-SPAM Act (the “Act”) defines a “commercial electronic mail message” (“CEMM”) as any electronic mail message, the primary purpose of which is commercial advertisement or the promotion of a commercial product or service (including content on an Internet web site operated for a commercial purpose). Transactional or relationship electronic messages are carved out of the definition of a CEMM and are defined as electronic mail messages sent to effectuate a commercial transaction, provide warranty information or notification of a change in features or status of an individual, provide information directly related to an employment relationship or benefit plan, or are provided in conjunction with a transaction involving the delivery of goods or services including product updates or upgrades that the recipient is entitled to receive under the terms of the transaction. Transactional or relationship messages are subject only to the Act’s provisions relating to deception.

The major provisions of the Act are as follows:

1. The Act criminalizes certain activities related to CEMMs where the sender of the email knowingly intends to deceive the recipient or acquires information, such as the recipient’s address, through deceptive means; and

2. Prohibits certain acts and provides certain requirements for the sending of CEMMs, and prescribes enforcement methodologies, including the enforcement of the Act by the State Attorneys General; and

3. Provides penalties for both the criminal acts and the civil wrongdoing; and

4. Provides mandates for future activities, including reports to Congress on a federal “Do Not Mail” registry.

Prohibited Activities

Prohibited Activities Relating to the Character of the Email. Section 105, entitled “Other Protections for Users of Commercial Electronic Mail” will have the widest commercial application in that it specifies certain prohibited acts relating to all CEMMs. The Section prohibits the following:

1. False or misleading transmission information in a CEMM or a transactional or relationship message, which is defined as information in the header of the email

that is materially false or misleading, including such header information that is technically accurate but has been obtained through false or fraudulent pretenses.

2. Deceptive subject headings in a CEMM where the initiator knows that the subject heading will mislead the recipient.

3. Sending a CEMM to a recipient that does not contain a functioning return address enabling the recipient to send a message declining future emails.

4. Sending a CEMM to a recipient who has notified the initiator that no such further emails are desired, including provisions that proscribe assisting an initiator in undertaking such activity, consciously avoiding receipt of the opt-out message or selling a list including the name of the recipient who has opted-out.

5. Sending a CEMM to a recipient without a clear and conspicuous identification that the email message is an advertisement or a solicitation, containing the clear and conspicuous notice of an opt-out procedure and containing a valid physical postal address of the sender.

6. Sending a CEMM to a recipient if the initiator actually knows, or knowledge can be implied, that the electronic email address of the recipient was obtained from a repository which prohibited such activity, or obtaining the address through other automated means.

7. The automated creation of multiple electronic email accounts for transmitting, relaying or retransmitting a CEMM that is unlawful under the first five prohibitions above.

8. Sending a CEMM that includes sexually oriented material without adequate warnings in the subject heading and an opt out message prior to displaying any additional information in the message.

Criminal Activities. Section 104, entitled “Prohibition Against Predatory and Abusive Commercial Email,” amends Chapter 47 of Title 18 of the United States Code, Section 107 and makes it a criminal act to:

1. Access a computer without authorization and intentionally initiate the transmission of multiple CEMMs from that computer;

2. Use a computer to relay multiple CEMMs with the intent to deceive or mislead the recipients or the Internet access service;

3. Materially falsify header information in multiple CEMMs and intentionally initiate the transmission of those messages;

4. Register, using information that materially falsifies an identity, for five or more electronic email accounts or two or more domain names and intentionally initiating multiple CEMMs from those accounts; or

5. Falsely represent the right to use five or more accounts and intentionally initiating multiple CEMMs from those accounts.

Companies Promoting Their Products Through Prohibited Activities. Section 106 of the Act makes unlawful the promotion of goods, products or services by a person through CEMMs which are prohibited under the deceptive practices provision (subsection (a)(1) of Section 105), if such person knew or should have known of the activity, received or is to receive an economic benefit, and took no steps to prevent it.

Enforcement And Penalties

The Act provides general enforcement powers by the Federal Trade Commission

as if a violation was an unfair or deceptive act or practice proscribed under the Federal Trade Commission Act. In addition, the Act allows other agencies of the federal government to enforce, with respect to entities and instrumentalities under their control, including the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Securities and Exchange Commission, the Federal Communications Commission, the Secretary of Agriculture, and others.

In addition, the Act allows the Attorneys General in the various states to bring civil actions in federal court for injunctive relief or damages where the Attorney General has reason to believe that any interests of the residents of the applicable state have been, or are being, threatened or adversely affected by someone engaging in practices violative of the Act. In such actions the penalties may be the monetary loss actually suffered by those residents or an amount calculated by multiplying up to \$250 times each violation relative to false or misleading transmissions. There is also an aggregate cap on damages in such actions of \$2 million. The Act also provides that Internet access services may bring a civil action in any United States district court with jurisdiction over the defendant for injunctive relief or damages calculated on the basis of \$100 per violation of the deceptive practices section and \$25 per violation of other sections to an aggregate cap of \$1 million.

The penalty for criminal violations of Section 104 is a fine and/or imprisonment for up to three years (five years for repeat offenders or violation in connection with a felony) and the forfeiture of any property used in the commission of the violations.

Preemption Of State Laws

Through November of 2003, approximately thirty-six states had passed some form of anti-SPAM legislation. The Act “supercedes any state statute, regulation, or rule of a State or a political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.” Hence, state legislation which legislates the fashion in which a CEMM can be sent or is labeled, or that requires opt-in or opt-out procedures is superceded by the Act. State legislation that prohibits falsity and deception in any portion of a CEMM is left standing. The Act also provides that it specifically does not preempt state laws that are not specific to electronic mail, including state trespass, contract, or tort laws, or those that relate to acts of fraud or computer crime. The federal preemption statement is supported by legislative findings in the Act that find that the patchwork of state legislation has been ineffective to stem the rise of SPAM on a national basis.

Miscellaneous Other Provisions

The Act also provides for the study and a report to Congress on the following areas:

1. A report to Congress from the FTC no later than six months after enactment on a plan and timetable for the establishment of a nationwide “Do Not Email” registry. This provision also allows the FTC to establish and implement such a plan no

earlier than nine months after the enactment of the Act.

2. A report to Congress no later than twenty-four months after the enactment of the Act on the extent of technological and marketplace developments and how they impact the provisions of the Act and a recommendation on how to address commercial email that originate in other nations.

3. A report within nine months after the date of the enactment of the Act on how to provide rewards for individuals who provide information leading to violators of the Act.

Strategies For Compliance

Businesses may wish to begin to separate the kinds of email messages initiated into the categories set up by the Act. Transactional and relationship messages are not considered CEMMs and are covered only by the deceptive practices provisions, for instance, and might comprise a category. This separate category may be of particular interest to companies whose websites already provide automatic confirmations of orders or reservations – messages that would clearly fall into the “transactional” category. As an ounce of prevention in such instances, customers might be advised that certain interactions, such as the sale of goods or services, are considered “transactions” under the Act and that follow-up emails will be initiated (without the requirements the Act sets up for CEMMs). An alternative, of course, would be to comply with all of the provisions of the Act as they relate to all messages.

On the other hand, many businesses may deem it too much of a burden to split the emails they send into the categories set out in the Act, particularly because such a strategy may well necessitate a legal conclusion as to each individual commercial message. An obvious alternative for companies ascribing to such a view would be to comply with all of the provisions of the Act as they relate to all electronic messages.

If a company works with a third party with regard to marketing activities, such parties should be notified in writing of the company’s position on compliance. Companies are also well advised to perform reasonable checks on these third parties to insure their continued compliance.

The Act also provides that if a company has established and implemented reasonable practices and procedures to effectively prevent violations and has undertaken a good faith attempt to maintain compliance with such practices and procedures, any penalty for violation will be decreased. In addition, other sections require actual knowledge, the existence of which would be limited by a well-drafted compliance policy. Therefore, it will be important to comply with the provisions of the Act relative to the ability to reply to commercial email messages, and to exercise the option to opt-out of such messages, but it will also be prudent for legitimate enterprises to establish a written compliance procedure in order to gird any defenses against unintended violations.

The approach taken by an individual business will vary based on commercial realities, but the best compliance practice might be to engage in all of the practices noted above, thereby setting up a series of protections. Since the effective date of the Act was January 1, 2004, businesses would be well advised to undertake compliance procedures as soon as possible.

Michael Siavage is a Partner in the Atlanta office of McKenna Long & Aldridge LLP. He focuses his practice on intellectual property transactions, commercialization of university intellectual property, mergers and acquisitions, advice to public companies on growth company creation and acquisition and the transactions connected with raising venture capital. He can be reached at msiavage@mckennalong.com.

Please e-mail the author at msiavage@mckennalong.com with questions about this article.