



CANNING SPAM

As most people probably know by now, Congress enacted the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) at the end of 2003 to federalize the law regarding commercial e-mail. The law was rushed through Congress in order to preempt a California law which was about to become effective. Federal action was welcome to many who were worried about the prospect of having to deal with different rules in different states with respect to an essentially borderless medium. Although state law may remain relevant for some purposes, Congress's action was a step towards uniformity in an area where some regulation was inevitable. The ensuing discussion will summarize the provisions of the Act and comment on its likely impact.

I. SCOPE OF CAN-SPAM ACT – COMMERCIAL ELECTRONIC MAIL MESSAGES

The Act has a broad reach and applies to all "commercial electronic mail messages." A commercial electronic mail message is "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service including content on an Internet website operated for a commercial purpose." Congress has directed the Federal Trade Commission to come up with rules to flesh out the definition of commercial e-mail by the end of this year. Pending the FTC's promulgation of these rules, however, it is probably advisable to construe the language broadly

Virtually all e-mails where the primary purpose is advertising or solicitation of business are covered by the Act; however, the CAN-SPAM Act contains an exception for transactional or relationship messages. Under the Act, transactional or relationship messages or commercial e-mails are messages intended (i) to facilitate, complete or confirm a commercial transaction that the recipient has previously agreed into with the sender, (ii) to provide warranty information, product recall information or the like or (iii) to provide notification concerning a change in the terms or features of or in the recipient's standing or status with respect to any subscription, membership or comparable ongoing commercial relationship. The relationship exception also covers information relating to employment relationships or benefit plans or relating to the delivery of goods or services the recipient is entitled to receive under the terms of a transaction the recipient had previously agreed to enter into. One may hope that further guidance as to the scope of the transactional/relationship exception will be part of the FTC rules.

Of course, as a general matter, it would appear that most e-mails transmitted in the ordinary course of business do not have advertising or solicitation as their primary purpose, and would therefore would fall outside the purview of the Act in the first instance. However, when the primary purpose is commercial advertisement or promotion of a commercial product or service, and the transactional relationship message exception does not apply, the Act must be complied with.

II. OPERATIVE PROVISIONS

The operative provisions of CAN-SPAM make it unlawful for any person to initiate the transmission of any commercial electronic mail message unless a message provides (i) clear and conspicuous identification that the message is an advertisement or solicitation, (ii) clear and conspicuous notice of the opportunity to decline to receive further commercial electronic mail messages from the sender and (iii) contains a valid physical postal address of the sender. The first requirement need not be met if the recipient has given prior affirmative consent to receipt of commercial e-mail from the sender. Although the Act does not go into any detail as to how to define clear and conspicuous, common sense would indicate that putting the required advertising disclaimer and opt-out provision in small print at the end of the e-mail attachment would not pass muster.

In addition to these three requirements, the Act delineates certain other restrictions. For example, e-mails including sexually-oriented material will be required to contain certain marks or notices in the heading for the electronic mail message, which marks and notices will be prescribed by the FTC. The Act also makes it a violation of Federal law to send messages with header information that is technically accurate, but materially false, such as an originating electronic mail address, the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses. It also will be a violation to knowingly use a subject heading which would be likely to mislead a recipient as to a material fact regarding the e-mail's content.

Service providers have some immunity under the Act as to the fraud type violations, but service providers are not protected if they own a 50% or more economic interest in the entity that violated the Act, and they provided the misleading information or had knowledge that the commercial electronic mail message violated the Act.

E-mails must contain a functioning return e-mail address or other Internet based mechanism, clearly and conspicuously present, to which a recipient can respond requesting that it not receive further commercial e-mail from such source. The e-mail may include a list or menu from which the recipient may choose not to receive e-mails of a certain type so long as there is an option which would allow the recipient to request not to receive any commercial messages at all from the source. The return e-mail message or Internet mechanism must remain capable of receiving messages or communications for not less than 30 days after the transmission of the original message.

The Act also prohibits "address harvesting" or "dictionary attacks." These practices are aggravated violations under the Act. Prohibited address harvesting is the process of obtaining electronic mail addresses by automated means from someone else's website or online service where such other person's website or online service indicates to the public that the operator of such website or service would not sell or transfer addresses maintained by such website or online service to another party. Dictionary attacks involve obtaining mail addresses by using automated means to generate possible electronic mail addresses by combining names, letters or numbers into numerous permutations.

Another prohibited activity is the use of scripts or automated means to register for multiple online user accounts to enable transmissions of commercial electronic mail messages which otherwise violate the Act.

Finally, the Act makes it unlawful for any person to knowingly retransmit an unlawful commercial email message from a computer that such person has accessed without authorization.

III. CONSENT

Consent of the recipient to receive commercial e-mail obviates the need to identify messages as advertisements or promotions. Under the Act, 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, or, if the message is from a party other than the party to which the recipient communicated such consent, the recipient was given clear and conspicuous notice at the time that the consent was communicated that the recipient's electronic mail address could be transferred to such other party for the purposes of initiating commercial e-mail messages.

IV. COMPLIANCE WITH RECIPIENT REQUESTS FOR RECORD OF NAME

The Act dictates that anyone doing mass e-mailings act promptly when receiving a request not to send further messages to a particular recipient. There is a 10-day grace period to remove a recipient's name from a mailing list after the recipient requests removal. Given this provision, it will obviously be important for companies using multiple e-mail lists to institute safeguards that will ensure that parties requesting that their names be removed are in fact removed from all mailing lists used by the company. Companies will also need to take care to prevent the names of people who have previously asked not to receive any more e-mail from being included in new lists when such lists are being developed.

V. DO NOT E-MAIL FEDERAL REGISTRY

The Can-Spam Act also directs the FTC to develop a Do Not E-Mail Federal Registry, which would presumably be similar to the Federal Do Not Call Registry. E-mail users will have to wait and see exactly what the FTC develops, but the creation of such a list could obviously have significant implications for anyone using the Internet e-mail for advertising or promotional purposes.

VI. ENFORCEMENT

While the passage of the CAN-SPAM Act may conjure up a specter of massive litigation clogging the courts, the enforcement provisions of the Act make this unlikely. First of all, there is no private right of action except for Internet service providers. Of course, a disgruntled consumer may notify the FTC, which could result in FTC action. It seems reasonable to assume, however, that the FTC will be concerned more with the true "spam" that beleaguers most PC users rather than incidental technical violations of the Act. The FTC may seek injunctive relief. The Act also allows a state attorney general to seek statutory damages calculated by multiplying the number of violations by up to \$250. Each separately addressed unlawful message received by or addressed to any person will be counted as a separate violation; however, total statutory damages may normally not exceed \$2,000,000. Internet service providers may seek damages which are subject to somewhat lower limits. A court may increase the damage award, however, to not more than three times the amount otherwise available where it determines that the defendant committed the violation willfully and knowingly

or the defendant committed a so-called aggravated violation such as address harvesting or a dictionary attack.

VII. IMPACT ON SPAM

Although the CAN-SPAM Act attacks some of the more offensive practices of big time spammers such as misleading source identification, failures to identify e-mails which contain sexually oriented materials and concealing promotional nature of an e-mail, some have questioned whether the law will be effective in substantially reducing the amount of spam that has become part of life on the Internet. Recent reports have questioned whether there was any fall off in the amount of spam since the beginning of the year. The Director of the FTC's Consumer Protection Bureau has noted that finding the spammers is not an easy process. One reason the amount of spam may not have declined is that many spammers often operate outside the borders of the U.S. It was probably inevitable that the Federal government would step in at some point in this area. Time will tell whether the quality of life on the Internet is improved by its actions.

“Taking Stock” is presented by Gould & Ratner’s Corporate/Commercial Group for general informational purposes only, is not intended as legal advice, and cannot substitute for advice of counsel. If you would like to speak with an attorney at Gould & Ratner regarding the topic presented in this article, please contact David Brown at 312/899-1694 or dbrown@gouldratner.com or John Washburn at 312/899-1609 or jwashburn@gouldratner.com.

For more Taking Stock’s, please visit http://www.gouldratner.com/resources/gr_takingstock.cfm.

*Professional rules in some jurisdictions may treat **Taking Stock** as advertising.*

"Taking Stock" is presented by Gould & Ratner's Corporate/Commercial Group for general informational purposes only, is not intended as legal advice, and cannot substitute for advice of counsel.

If you would like to speak with an attorney at Gould & Ratner regarding the topic presented in this article, please contact David Brown at 312/899-1694 or dbrown@gouldratner.com or John Washburn at 312/899-1609 or jwashburn@gouldratner.com.