AVOIDING LIABILITY UNDER THE CAN-SPAM ACT OF 2003 FOR SENDING COMMERCIAL EMAIL

Background

The provisions of the act entitled "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003," better known as the "CAN-SPAM Act of 2003" (the "Act"), took effect January 1, 2004. The Act seeks to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial email, commonly known as "spam." The Act preempts state laws that are in some ways more restrictive. Unlike some state anti-spam laws, the CAN-SPAM Act does not prohibit commercial email or email advertising. The Act instead prohibits fraudulent and misleading email, and requires senders of commercial email to allow recipients to "opt out" of future mailings. Penalties for violations include fines, imprisonment and forfeiture of property. The Act is ambiguous in some respects and contains several specific pitfalls that should be kept in mind when establishing email policies.

Important Definitions

The CAN-SPAM Act applies primarily to commercial electronic mail messages ("CEMMs"), defined as email messages "the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet Web site operated for a commercial purpose)." However, the Act does not quantify what portion or quantity of an email must be "commercial advertisement or promotion" to qualify as a CEMM. An email could, for example, fall outside the definition by putting its advertising or promotional content in a postscript to a general friendship letter. Apparently anticipating such possibilities, the Act also empowers the FTC to issue by January 1, 2005 "regulations defining the relevant criteria to facilitate the determination of the primary purpose" of an email message.

The Act explicitly states that "transactional or relationship" messages are not CEMMs, and are therefore not subject to most provisions of the Act. The primary purpose of transactional or relationship messages is to complete a preexisting commercial transaction or further a pre-existing relationship between the sender and the recipient of the email.[1] The Act further

[1] Specifically, the primary purpose of a transactional or relationship message is: "(i) to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender; (ii) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient; (iii) to provide (I) notification concerning a change in the terms or features of, (II) notification of a change in the recipient's standing or status with respect to, or (III) at regular periodic intervals, account balance information or other type of account statement with respect to, a subscription, membership, account, loan, or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender; (iv) to provide information directly related to an employment relationship or related benefit plan in which the recipient

empowers the FTC to modify the definition of transactional or relationship messages to accommodate changes in email technology or practices and accomplish the purposes of this Act.

Prohibited Fraudulent Email Activity

The Act broadly prohibits actions by any sender and its conspirators to conceal the origin or subject of CEMMs. The Act further prohibits accessing a protected computer[2] without authorization, and intentionally initiating the transmission of multiple[3] CEMMs from or through such computer. This includes using a computer to relay or retransmit multiple CEMMs, with the intent to deceive or mislead a recipient or any Internet access service, as to the origin of such messages. Materially falsifying header information[4] in a CEMM, or even in a transactional or relationship message, and initiating the transmission of such a message is also prohibited under the Act.

Materially falsifying one's identity when registering for five or more email accounts or online user accounts or two or more domain names, and intentionally initiating the transmission of multiple CEMMs from any combination of such accounts or domain names, is prohibited. Falsely representing oneself to be the registrant of five or more Internet Protocol addresses, and intentionally initiating the transmission of multiple CEMMs from such addresses, is also prohibited.

Other Protections for Recipients of CEMMs

Every CEMM must contain a clear, accurate and conspicuous identification that the message is an advertisement or solicitation, and a valid physical postal address of the sender. The Act requires the FTC to submit a plan to Congress by June 1, 2005 for further requiring the use of characters such as "ADV" in the subject line of all CEMMs.

---

is currently involved, participating, or enrolled; or (v) 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." 18 U.S.C. § 1037.

[2] A "protected computer" is a computer "used in interstate commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate commerce or communication of the United States," 18 U.S.C. 1030 (e)(2)(B), which is, effectively, any computer capable of sending and receiving email or data across state lines.

[3] "Multiple" means more than 100 email messages during a 24-hour period, more than 1,000 email messages during a 30-day period, or more than 10,000 email messages during a one-year period. 18 U.S.C. § 1037(d)(3).

[4] "[H]eader 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 or to investigate the alleged violation." 18 U.S.C. § 1037(d)(2).

In addition, every CEMM must contain a functioning, clear and conspicuous return email address or other Internet-based mechanism that allows a recipient to opt out of future CEMMs from that sender. The return email address must remain capable of receiving such opt-out messages for no less than 30 days after the transmission of the original CEMM. The Act provides a ten-day grace period for the sender to process the recipient's opt-out request. If the return email address is unexpectedly and temporarily unable to receive messages or process opt-out requests due to a technical problem beyond the control of the sender, it is not considered a violation of the Act so long as the problem is corrected within a reasonable time period.

The person initiating a CEMM may comply with the opt-out requirement by providing the recipient a list or menu from which the recipient may choose the specific types of CEMMs the recipient wants does not want to receive from the sender. The list or menu, however, must include an option for the recipient to choose not to receive *any* CEMMs from the sender.

Once the recipient has opted out of receiving future mailings, it is unlawful for the sender (or any person acting on its behalf) to initiate or assist in initiating the transmission of CEMMs to the recipient, unless the recipient later rescinds the opt-out request. However, the Act does require that, to be liable, the sender must have actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such CEMMs would violate the opt-out requirements of the Act.

It is also unlawful for the sender, or any person who knows the recipient opted out, to sell, lease, exchange or otherwise transfer or release the email address of the recipient (including mailing lists bearing the email address of the recipient) for any purpose other than compliance with the Act or other provision of law.

The Act also enumerates several aggravated violations relating to automated address harvesting and dictionary attacks,[5] automated creation of multiple email accounts, relaying or retransmission through unauthorized access, and lack of warning labels on CEMMs containing sexually oriented material. The FTC and the U.S. Attorney General are empowered to prescribe by April 30, 2004 clearly identifiable marks or notices for CEMMs that contain sexually oriented material.

Enforcement/Penalties

The FTC generally enforces the Act's provisions through the Federal Trade Commission Act (15 U.S.C. 41, *et seq*.), but several other agencies also have enforcement power under various other laws.

---

[5] This includes obtaining email addresses through automated means from an Internet Web site or proprietary online service that includes a notice stating that the operator will not give, sell or otherwise transfer addresses, and using an automated means to generate email addresses by randomly combining names, letters or numbers.

The Act may also be enforced against any person who knowingly promotes, or allows the promotion of, that person's trade or business in a CEMM that contains false or misleading transmission information, and receives or expects to receive an economic benefit from the promotion. Such persons are required to take affirmative action to prevent the CEMM or detect and report it to the FTC.

The maximum penalties for violations of the Act include fines and/or imprisonment for up to five years if the offense is committed in furtherance of any felony, or the defendant has previously been convicted under the Act or under the laws of any state for conduct involving the transmission of multiple CEMMs or unauthorized access to a computer system. Conviction of an offense under the Act also results in forfeiture of any property obtained from committing the offense, as well as "any equipment, software, or other technology used or intended to be used to commit or facilitate the commission of such offense."

The Act immunizes third parties such as Internet service providers for providing goods and services to other persons who violate the Act, so long as the third party does not own greater than 50 percent of the trade or business of the entity that violates the Act, have actual knowledge of the violation, or receive or expect to receive an economic benefit from the promotion.

A state attorney general may bring a civil action under the Act on behalf of the residents of the state. Statutory damages are calculated by multiplying the number of violations (messages received by or addressed to residents of the state) by up to $250, the total not to exceed $2,000,000. In cases where the violation is false or misleading transmission information in a CEMM or even a transactional or relationship message, there is no statutory damages limit.

An Internet access service provider may also bring a civil action to enjoin further violations or to recover damages for actual monetary loss incurred as a result of the violation, or statutory damages, whichever are greater. The statutory damages are calculated by multiplying the number of violations (unlawful messages transmitted or attempted to be transmitted) by up to $25, the total not to exceed $1,000,000. In cases where the violation is false or misleading transmission information in a CEMM or even a transactional or relationship message, each violation is multiplied by $100 and there is no statutory damages limit.

In either civil action described above, the Act allows aggravated damages of up to three times the amount otherwise available if the court determines that the defendant committed the violation willfully and knowingly, or the unlawful activity included one or more of the aggravating violations described above. Damages may be reduced if the defendant has established and implemented commercially reasonable practices and procedures designed effectively to prevent such violations. The court may also award the costs of the action and reasonable attorneys' fees to the prevailing state or Internet access provider.

Congress seeks to improve enforcement by rewarding people who report violations of the Act with a minimum of 20 percent of the total civil penalty collected. The Act requires the FTC to submit a report to Congress by June 1, 2005, detailing procedures for such a reward program. The FTC, in consultation with the Department of Justice and other appropriate agencies, must

also submit a report to Congress by January 1, 2006 that provides a detailed analysis of the effectiveness and enforcement of the provisions of this Act and the need (if any) for Congress to modify it. In an attempt to keep pace with ingenious methods of "repackaging" spam so it is in compliance with the letter, if not the spirit, of the Act, Congress also expects the FTC to analyze and recommend how to address CEMMs that originate in other nations.

Do-Not-Email Registry

The Act requires the FTC to submit by June 1, 2004 a report addressing the establishment of a nationwide marketing "Do-Not-Email Registry." The FTC may establish and implement the registry as early as September 1, 2004. The Do-Not-Email Registry would likely be similar to the Do-Not-Call Registry, which has been very popular as a curb to telephone solicitations. Interestingly, registration on the Do-Not-Call Registry is only possible using email.

Application to Wireless Communications

The advent of text messaging and email by mobile phones has made mobile users a target of spam as well. The Act requires the FCC, in consultation with the FTC, to promulgate rules by September 27, 2004 to protect consumers from unwanted mobile service commercial messages. The FCC must provide mobile subscribers the ability to avoid receiving mobile service commercial messages unless the subscriber has provided express prior authorization to the sender, and allow recipients of mobile service commercial messages to opt out of receiving future messages. The rules must also determine whether providers of mobile services should be subject to the same rule. Alternately, the rules shall require such providers, in addition to complying with the other provisions of the Act, to allow subscribers to indicate a desire not to receive future mobile service commercial messages from the provider.

Avoiding Liability Under the Act

To avoid liability under the Act and current regulations, companies sending commercial email should:

- Use accurate header information on all email messages;
- Clearly and conspicuously identify every CEMM as a promotion or advertisement and include the sender's valid postal address;
- Register domain names only in the names of actual persons or entities;
- Include in each CEMM a functioning, clear and conspicuous return email address with an option for the user to opt out of receiving future email;
- Within ten days of receiving an opt-out message, cease sending commercial email to the user unless that user later rescinds the opt-out instructions;

- Not sell, lease or otherwise transfer the email address of a user who has opted out of receiving further commercial email; and

- Not employ automated address harvesting or an automated method of creating email accounts.

* * * * * * * * * * * * * * *

If you have any questions concerning this memorandum, please contact William M. Ried (212-728-8729, wried@willkie.com) or Spyros Loukakos (212-728-8726, sloukakos@willkie.com).

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is 212-728-8000, and our facsimile number is 212-728-8111. Our Web site is located at www.willkie.com.

April 21, 2004