

(December 5, 2003)

A PRIMER FOR THE CAN-SPAM ACT OF 2003

The CAN-SPAM Act of 2003 is within a breath of passage. The Senate unanimously passed the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003," or "CAN-SPAM Act" on November 25, 2003. The House is expected to act on it in a matter of days, clearing the way for the first federal anti-spam law to be enacted before the end of the year. We provide this primer on the new law, recognizing that there is a slight chance that the law may not be enacted or may be modified before final passage.

GENERAL OVERVIEW

The Act provides both criminal and civil penalties for the unlawful transmission of unsolicited commercial email. Importantly, the Act will preempt the 37 existing state laws regulating commercial email -- including California's stringent SB 186 -- except to the extent such laws regulate false or deceptive emails.

Understanding the CAN-SPAM Act is important to companies that:

- Use email to communicate with existing or potential customers;
- Use third-party email lists to reach potential customers;
- Use viral marketing or referral campaigns, such as affiliate programs;
- Send commercial email on behalf of others; or
- Compile email address lists to share, rent or sell to others.

Overall, the CAN-SPAM Act is relatively business-friendly, providing a safe path for companies to communicate with their customers and prospective customers via email. The Act does not apply to a broad array of "transactional or relationship messages" whose "primary purpose" is non-commercial, such as recall notices, health and safety information, or customer service. For all unsolicited messages, advertisers and email marketers must identify the advertisement and themselves within the message and provide a mechanism for recipients to opt-out of receiving

future mailings. Email marketers cannot "harvest" addresses from the Internet or use other automated means of creating email lists. In addition, the Act criminalizes some of the most egregious spamming tactics, such as falsified header information, unauthorized use of others' computer facilities to send spam and other deceptive practices.

The Act vests the Federal Trade Commission with primary responsibility for enforcement and tasks the FTC with additional rulemaking to implement the Act. In addition, the Act mandates further studies and reports related to spam, including requiring the FTC to prepare a plan for establishing a nationwide marketing Do-Not-E-Mail registry within six months of its enactment. State Attorneys General and Internet Service Providers have only limited causes of action and private individuals who receive spam have no right of action at all under the Act.

If signed by the President, the Act will become effective January 1, 2004.

KEY PROVISIONS OF THE CAN-SPAM ACT

(1) Preemption of State Laws. The CAN-SPAM Act preempts any State statute, regulation or rule that "expressly regulates the use of electronic mail to send commercial messages," except to the extent that such laws prohibit falsity or deception in any portion of a commercial email message or attachment. Thus, the confusing and inconsistent state laws related to the form and content of email advertising are now preempted, as are the varying exceptions to their application, in favor of a uniform standard. State Attorneys General, however, may still prosecute certain fraudulent or deceptive email practices or other computer crimes under their own state laws and the Act does not impact any state laws not specific to electronic mail (such as trespass or contract).

(2) No Deceptive Ads or Transmissions. The Act provides strong criminal and civil penalties for accessing computers or using computers to relay or retransmit commercial email without authorization, falsifying header information or otherwise using false information to facilitate the sending of

commercial email, using deceptive subject lines and failing to place warning labels on email containing sexually oriented material.

(3) Opt Out Required. The Act requires that email marketers include in each commercial email a return address or some other "opt-out" mechanism for recipients to request not to receive future mailings. Once such a request is made, the advertiser may not initiate an email ad more than 10 business days after the receipt of such a request. Moreover, agents of the sender or list providers with actual knowledge, or knowledge fairly implied on the basis of objective circumstances that a particular message falls within the scope of a recipient's request must not initiate such transmissions. For larger companies that manage multiple email databases, it is possible to identify different departments or divisions as the source of email and to effect an opt out on a departmental basis.

(4) Identification of Ads and Advertisers. Like many of the current state laws, the CAN-SPAM Act requires that unsolicited commercial messages be clearly and conspicuously identified as advertisements, provide an opt-out mechanism as described above, and include the sender's physical postal address. Unlike many of the state laws, however, the Act does not require that "ADV:" or any other prescribed mark or notice be included in the subject line or text of the message. These content requirements do not apply if a recipient has given "affirmative consent" to receive such messages. Affirmative consent exists if a 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."

(5) Exception for "Transactional or Relationship Messages." The Act's opt-out and identification requirements do not apply to a broad category of email communications called "transactional or relationship messages." These include messages (a) to facilitate, complete, or confirm a transaction; (b) to provide warranty information, product recall or safety or security notices; (c) to provide notices concerning a change in subscription terms, standing or status or account information; (d) regarding employment or benefits information; or (e) to deliver goods or services pursuant to a prior

transaction, such as software upgrades or patches. As such, most customer communications will be exempt from the Act's content requirements. It remains unclear, however, whether and/or when *former* customers may be contacted.

ENFORCEMENT

Criminal Prosecution. The Act encourages the Department of Justice to "use all existing law enforcement tools to investigate and prosecute those who send bulk commercial e-mail to facilitate the commission of Federal crimes." To that end, the criminal provisions in Section 4 of the Act for predatory and abusive email practices are accompanied by stiff penalties, including fines, forfeiture of proceeds and equipment used in the offense, and up to five years in prison.

FTC Enforcement. Violation of the Act is also an unfair or deceptive practice under the Federal Trade Commission Act, and thus violators may be subject cease and desist orders, injunctions and civil penalties up to \$11,000 per violation. The Act also authorizes enforcement by certain other federal regulators against entities outside of the FTC's jurisdiction (e.g., banks, credit unions, broker-dealers, insurers, common carriers, etc.)

State Enforcement. The Act authorizes State Attorneys General and other appropriate state agencies to bring an action on behalf of their residents. The States may obtain injunctive relief, or statutory damages for up to \$250 per violation, capped at \$2 million for any violation other than false or misleading headers. Damages may be trebled for willful violations and, importantly, damages may be reduced if the defendant can demonstrate that it has established and implemented reasonable practices to prevent violations. In addition, the States may continue to bring criminal actions based on state anti-fraud or computer crime laws that are not preempted by the Act.

ISP Actions. Internet Access Service Providers may also bring an action for transmitting false or misleading header information, address harvesting or

dictionary attacks or other unauthorized use of email accounts for the purpose of sending spam, failing to place warning labels on email containing sexually oriented material, or a pattern and practice of failing to respect opt-out requests. ISPs may obtain injunctive relief, actual damages or statutory damages of up to \$100 per violation for sending fraudulent or deceptive spam under Section 5(a)(1) and up to \$25 for each other violation up to \$1 million. Damages may be trebled for willful conduct and damages may be reduced if the defendant has implemented a reasonable program to prevent violations. Spam recipients have no private right of action.

IMPORTANT RULEMAKING & REPORTS TO COME

Further Rulemaking. The Act directs the FTC to issue further regulations for:

Determining the "primary purpose" of a commercial email message.
(Within 12 months of enactment.)

Expanding or contracting the categories of messages treated as "transactional or relationship messages," if appropriate.

Modifying the 10-business-day period for complying with opt-out requests, if appropriate.

Specifying additional activities or practices that contribute substantially to the proliferation of illegal spam and should be prohibited.

Labeling Commercial Email. No later than 120 days after enactment, the FTC -- in consultation with the Attorney General -- must prescribe clearly identifiable marks or notices to be included in or associated with commercial email that contain sexually oriented material. In addition, within 18 months of enactment, the FTC must submit a recommendation for requiring commercial email to be identifiable from its subject line by use of ADV or other method.

Do-Not-Email Registry. The FTC is required to produce a report to Congress within six months of the enactment of the Act that (a) sets forth a plan and timetable for establishing a nationwide marketing Do-Not-E-Mail registry; (b) includes an explanation of any practical, technical, security, privacy, enforceability or other concerns regarding such a registry; and (c)

includes an explanation of how the registry would be applied with respect to children with email accounts.

Wireless Messaging. The Federal Communications Commission, in consultation with the FTC, shall promulgate rules within nine months to protect consumers from unwanted mobile service commercial messages, taking into account the limitations on the size of text messages and the form factors of wireless devices.

"Rewards" Leading to Violators. Within nine months of enactment, the FTC must submit a report setting forth a system for rewarding those who supply information about violators.

Report to Congress. Not later than 24 months after enactment, the FTC shall submit a report to Congress on the effectiveness and enforcement provisions of the Act and recommend any modifications.

RECOMMENDED ACTIONS

Companies that use email to communicate with existing or potential customers should prepare and implement an internal policy for handling commercial email. Such a policy should include:

Content requirements for all commercial email that include identification of the ad and the advertiser (with physical mailing address), unless the recipient has provided affirmative consent to receive such messages.

An opt-out mechanism for all commercial email that remains functioning for at least 30 days after sending the email.

A process for managing opt-out requests to ensure that no commercial email are sent 10 business days after a request is received. This process should take into consideration any affiliates or third parties that send out email on your behalf. This may not be a trivial IT task and companies should begin checking now.

List brokering still faces challenges under the Act as was the case under California's tough anti-spam law. List acquirers will want to have assurances that lists are "fresh" and that all opt outs older than 10 business

days are suppressed. Further, list acquirers will want representations that the lists were not compiled by harvesting sites without permission.

Training of staff who handle commercial email regarding the Act, including the provisions related to deceptive transmission and content.

This Update is not legal advice nor is it intended to apply to any specific facts or circumstances. Updates are provided periodically by Perkins Coie LLP as a service to our clients and friends. If you prefer not to receive Updates in the future, please reply to the message with "unsubscribe" in the subject line. If you have any questions about this Update, please email: Al Gidari, agidari@perkinscoie.com; Nicole Wong, nwong@perkinscoie.com; nwong@perkinscoie.com Kurt Opsahl, kopsahl@perkinscoie.com; Suchon Tuly, stuly@perkinscoie.com.

Perkins Coie LLP (Perkins Coie LLC in Illinois)