February 20, 2004


On December 16, 2003, President Bush signed the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, known as the CAN-SPAM Act. The new law, which became effective on January 1, 2004, establishes a framework for federal regulation of unsolicited commercial e-mail, expressly preempts inconsistent state anti-spam law (including California’s newly adopted opt-in law).

The CAN-SPAM Act does not ban spam. Instead, it prohibits certain deceptive and fraudulent e-mail practices and requires senders to include appropriate subject headings and an “opt-out” mechanism for recipients. The CAN-SPAM Act also requires the Federal Trade Commission to report on adoption of a national “do-not-spam” list (similar to the “do-not-call” list) and other possible extensions of federal spam regulation.

The CAN-SPAM Act provides for criminal penalties as well as civil enforcement by the FTC and state attorneys general. It permits Internet service providers to bring private actions to enjoin violations or recover damages, but does not create private rights of action for individual spam recipients.

Scope of the CAN-SPAM Act

The prohibitions and requirements of the new law apply to any “commercial electronic mail message.” The term is broadly defined to include any e-mail that has as its “primary purpose” the “commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose).” The FTC is required to issue regulations defining “primary purpose” by January 1, 2005.

Expressly excluded from the definition (and from CAN-SPAM prohibitions and requirements, other than the prohibition on false or misleading header information) is any “transactional and relationship message.” A “transactional and relationship message” is an e-mail whose “primary purpose” is to (1) facilitate, complete or confirm commercial transactions previously agreed to by the recipient; (2) provide warranty, product recall, safety or security information regarding products or services used or purchased by the recipient; (3) provide notice of change in terms or features, or recipient’s standing or status, or periodic account information relating to a subscription, membership, account, loan or comparable commercial relationship, involving the ongoing purchase or use of sender’s products or services; (4) provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved; or (5) deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under a transaction previously agreed to by the recipient. The FTC may modify this definition by regulation to accommodate changes in e-mail technology or practices.
Until there is further guidance from the FTC, the breadth of “commercial electronic mail message” and the narrowness of the “transactional and relationship message” exception will require businesses to consider carefully whether e-mails – even those not normally considered spam – must comply with the prohibitions and requirements of the CAN-SPAM Act. Examples of e-mails that may fall within the scope of the new law include: advertisements for future product releases (if the customer has not purchased ongoing maintenance services automatically entitling them to such new releases), newsletters, invitations to seminars or events, notices of sales or discount offers or other general information about the products or services offered by a business. In each case, businesses must assess whether the “primary purpose” of the communication is “commercial advertisement or promotion.”

The CAN-SPAM Act prohibitions and requirements, as well as potential criminal and civil liabilities, apply to third-party e-mail marketing firms; in fact, the businesses that hire them may be held liable for any violations committed by such firms. Further, the new law applies regardless of whether the “commercial electronic mail message” is being sent to one or thousands of individuals.

**Prohibitions and Requirements of the CAN-SPAM Act**

**False or Misleading Header Information.** With respect to both “commercial electronic mail messages” and “transactional and relationship messages,” the new law prohibits any attempt to use a false or misleading means to conceal the identity of the sender. Examples of prohibited acts include unauthorized use of a computer to initiate transmission of e-mails, retransmission of e-mails through various computers in order to deceive or mislead recipients regarding the origin of the e-mail and falsification of the header information (such as the “from” line).

**Deceptive Subject Lines.** The new law prohibits use of a subject heading in any “commercial electronic mail message” that is likely to mislead a recipient about the contents or subject matter of the message.

**Mandatory Opt-Out.** The new law requires all “commercial electronic mail messages” to contain a return address (or other Internet-based mechanism) to allow recipients to opt-out from getting any further e-mails from that sender. The opt-out offer must last for 30 days from the date of sender’s e-mail. If a recipient opts out, the sender must act within 10 days to prevent that recipient from receiving any more such messages. Once a recipient opts out, it is unlawful to sell, lease, exchange or otherwise transfer the recipient’s e-mail address for any purpose other than compliance with the CAN-SPAM Act or other law.

**Physical Postal Address.** The CAN-SPAM Act requires that any “commercial electronic mail message” include a valid physical postal address of the sender.

**Identification as Advertising or Solicitation.** The new law requires a “commercial electronic mail message” to include a “clear and conspicuous identification that the message is an [a]dvertisement or [s]olicitation,” but it does not (as of yet) require (as some current state laws do) that it carry any specific notation such as “ADV” in the subject line.

**Labeling and Limitations on Sexually Explicit Material.** The new law requires the FTC to prescribe standardized and specific marks or notices to be used in the “subject” heading of any “commercial electronic mail message” that contains sexually explicit material. In addition,
sexually explicit content may not be included in the initially viewable portion of such an e-mail absent further action of the recipient.

**Aggravated Violations.** The CAN-SPAM Act further bans “aggravated violations,” including so-called dictionary attacks,\(^1\) harvesting of e-mail addresses,\(^2\) use of computer programs to create multiple e-mail accounts at random and the unauthorized use of another person’s computer to relay otherwise unlawful commercial e-mails. Aggravated violations can lead to trebling of civil penalties in state attorneys general enforcement actions as well as award of attorney’s fees.

**Preemption**

When the CAN-SPAM Act was adopted, more than 35 states had already enacted anti-spam legislation. Because Congress was conscious that different states had taken different approaches to regulation, the CAN-SPAM Act expressly preempts inconsistent state law provisions, including California’s stringent “opt-in” law, S.B. 186. The California law, which also became effective on January 1, 2004, would have barred sending any unsolicited commercial e-mail to any recipient in California unless the recipient had given prior consent. Many other existing state statutes provide aggrieved consumers a private right of action that will now also, presumably, be preempted by the CAN-SPAM Act. The CAN-SPAM Act does not, however, affect or change state laws that prohibit falsity or deception in commercial e-mails or attachments, and it does not preempt any state laws that are not specific to e-mail.

**Further Reports and Studies**

The FTC must submit to Congress by July 1, 2004, a report setting forth a plan and timetable for establishing a “do-not-e-mail” registry. The CAN-SPAM Act also requires the FTC to report by October 1, 2004, on a potential reward system for persons who provide data on violations of the new law. It also requires the FTC to establish a plan by July 1, 2005, requiring commercial e-mail to be more readily identifiable through use of an “ADV” or similar label in its “subject” line. The new law also requires the Federal Communications Commission to publish regulations on application of the law to wireless devices, such as cellular telephones, by October 1, 2004.

Finally, the FTC (in consultation with the Department of Justice and other appropriate agencies) must submit to Congress by January 1, 2006, a detailed analysis of the effectiveness and enforcement of the CAN-SPAM Act.

**Conclusion**

Whether the CAN-SPAM Act will have a salutary effect on the scourge of unwanted commercial e-mails is far from clear. Disreputable businesses that regularly send out vast quantities of

---

\(^1\) In a dictionary attack, a hacker tries to determine a legitimate user’s password by using every “word” in a “dictionary” of plausible passwords. Once found, the hacker uses the password to gain unauthorized access to the user’s network and data. Dictionary attacks succeed because many user passwords are taken from common words, names or combination of words and names with only minor changes that the user finds easy to remember.

\(^2\) A spammer may “harvest” or collect e-mail addresses from the Internet by automatically scanning chat rooms where users disclose their e-mail addresses, by using so-called “blogs” that automatically scan the Internet or by other means of unauthorized collection and compilation.
unsolicited spam may be expected to take steps to evade the reach of the new law. Legitimate businesses, on the other hand, may find that the new law hinders the flow of commercial, marketing and other customer service communications of a type few would consider to be spam, due to the broad scope of the new law’s application.

About Dorsey & Whitney
Clients have relied on Dorsey since 1912 as a valued, cutting-edge business partner. With over 670 lawyers in 20 locations in the USA, Canada, Europe and Asia, we provide an integrated, proactive approach to our clients’ legal and business needs. Dorsey represents a number of the world’s most successful Fortune 500 companies from a variety of disciplines including leaders in the financial services, investment banking, life sciences, securities, technology and energy sectors, as well as nonprofit and government entities.

©2003 Dorsey & Whitney LLP. This Corporate Update is intended for general information purposes only and should not be construed as legal advice or legal opinions on any specific facts or circumstances. Members of the Dorsey & Whitney LLP Corporate Group will be pleased to provide further information regarding the matters discussed in this Corporate Update.