JONES DAY COMMENTARIES

February 2004

Technology Commentaries: The Federal CAN-SPAM Act — New Requirements for Commercial E-Mail

After six years of debate, Congress finally passed "anti-spam" legislation in December 2003. The Act, entitled the Controlling the Assault of Non-Solicited Pornography and Marketing Act, better known as the CAN-SPAM Act, became effective January 1, 2004. The Act sets forth a much-needed set of national requirements for commercial e-mail and generally preempts state anti-spam laws, although the exact scope of preemption may well be the subject of future litigation. Under the Act, companies will be able to conduct e-mail marketing campaigns without fear of running afoul of inconsistent state laws.

Significantly, the Act does not ban spam per se. Instead, it prohibits deceptive or misleading commercial e-mail, requires senders to provide recipients with the ability to "opt out" of future mailings, and imposes a variety of other requirements discussed below. Additionally, the Act requires the Federal Trade Commission to evaluate the creation of a do-not-spam registry similar to the national do-not-call registry, which was established in response to consumer complaints about telemarketers.[1]

The CAN-SPAM Act provides for severe civil and criminal penalties for noncompliance, including statutory damages up to $6 million for willful violations and, in some cases, prison terms of up to five years. The Act does not provide for a private right of action by recipients of spam, but does authorize the federal government, state attorneys general, and Internet service providers to bring actions against violators.[2]

Businesses that engage in direct e-mail marketing (including wireless messaging) should review their marketing practices for compliance with the Act to avoid what could be substantial financial exposure as well as brand damage that can arise from noncompliance. Companies that operate globally must also consider compliance with international requirements, particularly the European Union Privacy and Electronic Communications Directive.

Impact of Spam

Companies that utilize commercial e-mail as a direct marketing tool have found it to be one of the most cost-effective ways to advertise. Literally with a "click," e-mail can reach millions of consumers at a modest cost and on a global level. Nevertheless, unsolicited commercial e-mail ("UCE," *i.e.*, spam) has become objectionable to many recipients and threatens to undermine the value of e-mail as a productive marketing and communication vehicle.[3] Spam also imposes significant tangible and intangible costs on Internet service providers, businesses, and consumer.

It is currently estimated that approximately 56 percent of all e-mail on the Internet is spam, and this figure is expected to

1 The Federal Communications Commission established the national do-not-call registry in 2003 under the Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2003).

2 The FTC can seek injunctions and fines up to $11,000 per violation, state attorneys general can seek damages up to $250 for each offense with a cap of $2 million (may be trebled for willful violations), and Internet service providers may seek damages of $100 per e-mail for e-mails with false headers and $25 per e-mail that violates other provisions of the Act.

3 Deborah Fellows, *Spam: How it is Hurting E-mail and Degrading Life on the Internet,* Pew Internet & American Life Project, Oct. 22, 2003. Fifty-two percent of e-mail users report spam made them less trusting of e-mail in general.

increase to 65 percent in 2004.[4] In 2003, spam cost businesses hundreds of millions of dollars annually in lost productivity, additional hardware to maintain e-mail transmission, and blocking and filtering software.[5] Indeed, the market for anti-spam services is expected to climb above $1 billion by 2008 from a little over $120 million in 2003.[6] Spammers also are often responsible for the spread of computer viruses, which can virtually shut down a business' network and directly affect productivity and revenue.

Finally, spam can pose a significant threat to the name and goodwill of a company as a result of "spoofing" — the hijacking of a legitimate company's name, e-mail address, or domain name and using it to disguise the source of the e-mail that is sent to consumers. Spoofing has become a preferred tactic for spammers because it allows them to bypass Internet service provider filters that recognize a legitimate company's name and thus trick consumers into opening an e-mail or buying counterfeit goods of a company.[7] In some cases, consumers respond to the spam message they believe originated from a legitimate company and unknowingly provide personal information the spammer then uses for financial gain.

Provisions of the CAN-SPAM Act

The CAN-SPAM Act does not ban spam but instead sets forth a set of national requirements for the use and transmission of any commercial e-mail. Companies that do not think of themselves as "spammers" nevertheless are subject to the Act if they use e-mail in their businesses. The requirements of the CAN-SPAM Act vary depending on whether the e-mail is categorized as a commercial e-mail message or a transactional or relationship e-mail message. A commercial e-mail message is any e-mail the primary purpose of which is the commercial advertisement or promotion of a commercial product or service. Commercial e-mail is the most heavily regulated category of e-mail. A transactional or relationship e-mail message is e-mail that is sent to facilitate an ongoing transaction or relationship and includes, among other things, providing information about employment relationships or related benefit plans, account balances, product recalls, upgrades, warranties, product safety, and subscriptions. Transactional or relationship e-mail is subject to fewer requirements than commercial e-mail.[8]

Compliance

The Act imposes the following obligations on companies, depending upon the category of e-mail that is transmitted:

- The sender is prohibited from using false information and deceptive subject lines and must include a "from" line that accurately identifies the sender of the e-mail.
- The sender must clearly and conspicuously identify unsolicited commercial e-mail as an advertisement or solicitation.
- The sender must include clear and conspicuous notice of the opportunity to opt out of receiving future e-mails and must provide an Internet-based reply mechanism by which recipients opt out, such as a return e-mail address or a link to a Web page from which the user can send an e-mail to contact the sender. This mechanism must remain operative for at least 30 days after the original message is transmitted.
- The sender, or anyone acting on behalf of sender, must stop sending e-mails to recipients within 10 business days after receiving an opt-out request.
- The sender must include a valid physical postal address of the sender.
- The sender is prohibited from using an automated means to harvest e-mail addresses from Web sites or online service providers that have policies of not sharing users' e-mail addresses.
- The sender is prohibited from using automated means to register for multiple e-mail accounts to be used to send spam.
- The sender may not use another person's e-mail or computer account to send commercial e-mail.
- The sender must include a warning label on unsolicited commercial e-mail containing sexually oriented material.

---

4 *Explosive Spam Growth Reveals More Criminal and Offensive Content.* Brightmail Web site press release: Spam Trends 2003.

5 Claudia Ray and Johanna Schmitt, "Stopping Spam: Federal and International Initiatives," Journal of Internet Law, November 2003.

6 Dan Thanh Dang, *Spammer Suspect Arrested in N.C.,* Dec. 12, 2003 at www.sunspot.net/technology/bal-bz.spam (Gartner, Inc. Market Research).

7 Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. §§ 7701-13 (2003); 18 U.S.C. § 1037 (2003), Report of the Committee on Commerce, Science and Transportation (S. 877), July 16, 2003.

8 Commercial e-mail sent to recipients who have previously consented to receive messages after a clear and conspicuous request or at the recipients' own initiative also is subject to fewer requirements under the CAN-SPAM Act.

The following chart summarizes certain of the differences in requirements based on whether e-mail is categorized as commercial, versus transactional or relationship:

	Commercial E-Mail Messages	Transactional or Relationship E-Mail Messages
False Header Information	Prohibited	Prohibited
Misleading Subject Line	Prohibited	Not Addressed
Opt-Out Notice/Opt Out Mechanism	Required	Not Required
Identification as Advertisement	Required (unless recipient has given prior consent to receive)	Not Required
Valid Physical Postal Address	Required	Not Required
Warning for Sexually Oriented Material	Required (unless recipient has given prior consent to receive)	Not Required

Best Practices for Commercial E-Mail

Developing a Company-Wide E-Mail Marketing Policy. Although not required by the Act, businesses should consider adopting a "best-practices" policy to implement the foregoing requirements and ensure consistency across business divisions and marketing groups. In addition, companies can be held liable for violations of the Act committed by vendors who send e-mail on the company's behalf if the company: (1) knows or should have known it is being promoted by spam; (2) is receiving or expects to receive an economic benefit from such promotion; and (3) takes no reasonable precautions to prevent such spam or to detect and report it to the FTC. Thus, a company should consider imposing its best-practices guidelines upon outside vendors as well as on company employees.

Maintaining an Opt-Out Database. Because the Act requires businesses to stop sending e-mail to consumers who opt out, companies should require employees and outside vendors to maintain a list of consumers who have opted out of receiving future e-mails and, obviously, take steps to ensure e-mail is not sent to recipients on that list. Companies and their outside vendors are responsible for adhering to each other's opt-out lists, and appropriate contract provisions should be adopted to ensure this occurs.

Purchasing or Renting Mailing Lists. The Act's prohibition on harvesting e-mail addresses has led to confusion about the purchase or renting of e-mail lists from third parties. The Act does not prohibit this traditional method of expanding a company's direct marketing activities, but the Act's requirements will apply to commercial e-mail sent from such lists. Consequently, companies acquiring such lists should consider seeking sufficient representations and warranties (with indemnification and other appropriate remedies) from the provider of such lists that: (a) the list was not created by means that violate the Act; (b) each recipient has been given clear and conspicuous notice that his or her e-mail address can be shared; and (c) each recipient has not opted out of receiving commercial e-mail. These provisions do not provide a "safe harbor" from liability under the CAN-SPAM Act, but rather provide some measure of recourse. Consequently, companies should exercise care in selecting third parties from which they acquire lists.

Federal Preemption

The Act generally preempts state anti-spam laws,[9] many of which imposed far more stringent requirements on use of commercial e-mail (including California's, which had mandated an opt-in requirement and allowed for private causes of action by consumers).[10] However, the Act does provide for two exceptions to state law preemption. First, the Act does not preempt state laws that "prohibit falsity or deception in any portion of an electronic mail message…." Because each state has its own definition of what is false or deceptive, this exception may be problematic for a company that relies upon the definitions in the federal Act. The Act also does not preempt state laws that are "not specific to electronic mail, including state trespass, contract and tort laws; or other state laws…relate[d] to acts of fraud or computer crime." This means that companies may still be subject to consumer, or Internet service provider, litigation if their direct marketing

9 Thirty-seven states had adopted anti-spam laws prior to enactment of the CAN-SPAM Act: Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Michigan, Missouri, Nevada, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, Wyoming.

10 Cal. Bus. & Prof. Code § 17529 (West 2003).

e-mail activities exceed certain bounds.[11] This may result in undermining one of the primary goals of the federal legislation, namely providing a uniform set of national guidelines for the transmission of e-mail.

International Anti-Spam Laws

Companies with cross-border e-mail marketing campaigns must also comply with international anti-spam laws that exist in 41 countries and the European Union. In an effort to address the inconsistencies in anti-spam laws of its member states, in July 2002 the European Union adopted the Privacy and Electronic Communications Directive, with implementation in each member state to be done by October 31, 2003.[12] The Directive includes commercial e-mail restrictions that are similar to the U.S. CAN-SPAM Act in that the Directive: (1) prohibits the use of false or misleading subject lines; (2) requires senders to include a valid reply address so that recipients can request that future e-mails be stopped; and (3) allows companies to transmit direct marketing e-mail to existing customers offering similar products or services on an opt-out basis. The Directive also includes commercial e-mail restrictions that are beyond those of the U.S. CAN-SPAM Act. Under the Directive, all commercial e-mail other than e-mail concerning similar products and services to existing customers is on an opt-in basis. One of the biggest challenges facing companies with widely varying product lines is determining whether they are allowed to operate on an opt-out basis with existing customers or whether the product differences mean that they are subject to the opt-in regime. In addition, unlike the U.S. CAN-SPAM Act, individuals have a private right of action to enforce the provisions of the Directive.

Conclusion

The CAN-SPAM Act's requirements for e-mail marketing are not universally supported. Supporters of the Act claim that by preempting disparate state anti-spam laws, the Act provides a much-needed national standard for e-mail marketing. Opponents argue that by preempting tougher state laws, the Act does little to decrease the amount of spam on the Internet and consistency of enforcement will not in fact occur. Indeed, companies must still seek to create e-mail direct marketing best practices that comply not only with federal law but, when applicable, international law as well. The good news is that compliance with the federal law should largely ensure that companies may now transmit commercial e-mail in the United States without significant risk.

Further Information

Technology Commentaries are a publication of Jones Day and should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at its discretion. The mailing of this publication is not meant to create, and receipt of it does not constitute, an attorney-client relationship.

For further information, readers are encouraged to contact their regular Jones Day attorney or any of the lawyers listed below. General e-mail messages may be sent using our Web site feedback form, which can be found at www.jonesday.com.

James Brelsford jfbrelsford@jonesday.com	Menlo Park	650-739-3944
Rachel Lerner rlerner@jonesday.com	Cleveland	216-586-7743
Kevin Lyles kdlyles@jonesday.com	Columbus	614-469-3821
Elizabeth Robertson erobertson@jonesday.com	London	44-20-7039-5204

11 For example, state trespass laws have been successfully used to pursue spammers. *See Hotmail Corp. v. Van$ Money Pie,* 47 U.S.P.Q.2d (N.D. Cal. 1998) (granting ISP preliminary injunction on grounds, inter alia, that unsolicited bulk e-mail constituted trespass to chattels); *CompuServe, Inc. v. Cyber Promotions, Inc.,* 962 F. Supp. 1015 (S.D. Oh. 1997) (same). *See also American On-Line, Inc. v. IMS,* 24 F. Supp.2d 548 (E.D. Va. 1998) (following *Compuserve* and granting plaintiff ISP summary judgment on Virginia common law trespass to chattels claim). *Cf. Intel Corp. v. Hamidi,* 30 Cal. 4th 1342 (2003) (trespass to chattels arising from transmission of a substantial volume of unsolicited e-mail requires evidence of an injury to its property or legal interest therein).

12 Council Directive 2002/58 EC of 12 July 2002 on Privacy and Electronic Communications, 2002 O.J. (L 201) 37-47.