CALIFORNIA BAR JOURNAL
OFFICIAL PUBLICATION OF THE STATE BAR OF CALIFORNIA
July 2004

CAN-SPAM really be stopped?

By Dana H. Shultz

Unsolicited commercial electronic mail — commonly called "spam" — is the bane of today's electronic existence. As long ago as 1999, a Gartner Group survey found that 83 percent of respondents disliked spam, 14 percent were neutral and only 3 percent liked spam. ("ISPs and Spam: The Impact of Spam on Customer Retention and Acquisition," www.brightmail.com/pdfs/gartner_rebuilt.pdf)

(Click to Enlarge)

The 108th Congress decided to do something about the problem. The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (usually referred to as the "CAN-SPAM Act of 2003" or "CAN-SPAM") took effect Jan. 1.

The act

CAN-SPAM has four main provisions, which together aim to make commercial e-mail (including commercial content on Web sites) more truthful, more transparent and more avoidable.

First, CAN-SPAM bans false or misleading e-mail header information. A message's "From," "To" and routing information must be accurate and must identify the sender. This requirement attacks the common spammer practice of disguising the source of a message.

Second, CAN-SPAM prohibits deceptive "Subject" information. Spammers often make up enticing subject lines, betting that the user will open a message that would be ignored if the description were truthful.

Third, CAN-SPAM requires that the message include an e-mail or other internet-based mechanism by which the recipient can opt out of receiving e-mail messages in the future. The sender must process the opt-out request within ten business days of receipt. Once a recipient has opted out, the spammer cannot provide that recipient's e-mail address to a third party (except to comply with CAN-SPAM or any other law).

Finally, CAN-SPAM requires that commercial e-mail clearly and conspicuously state that it is an advertisement or solicitation and that the recipient may opt out of receiving commercial e-mail in the future. Furthermore, commercial e-mail must include the sender's postal address.

In addition to the foregoing, CAN-SPAM has brief provisions — and calls for Federal Trade Commission rulemaking — regarding e-mail depicting sexually explicit conduct and commercial e-mail messages to mobile wireless devices.

Enforcement and penalties

The FTC is authorized to enforce CAN-SPAM, and the Department of Justice is authorized to enforce criminal sanctions. In addition, other federal and state agencies may enforce the law against organizations under their jurisdiction, and internet service providers (ISPs) may sue violators.

Statutory damages can go as high as $2 million ($1 million for suits by ISPs), subject to trebling for willful and knowing violations and certain aggravated violations (e.g., harvesting addresses from Web sites), plus attorney fees.

E-mail recipients other than ISPs do not have the right to bring suit under CAN-SPAM. For Californians, this limitation may seem ironic and unfortunate. California was set to implement at

the beginning of this year an anti-spam law that was more stringent than CAN-SPAM (effectively requiring recipient opt-in before commercial e-mail could be sent) and included a private cause of action for spam recipients. CAN-SPAM preempts state anti-spam legislation, however, so the California law never took effect.

CAN-SPAM's criminal penalties may include fines; imprisonment for up to five years, depending on the nature of the offense and any prior convictions; and forfeiture of gross proceeds obtained from the offense as well as equipment, software and other technology used in committing the offense.

Uncertainty

One of the greatest challenges in complying with CAN-SPAM is figuring out exactly which communications are covered. Most of the act addresses "commercial electronic mail messages," which means any message "the primary purpose of which is the commercial advertisement or promotion of a commercial product or service."

Commercial messages expressly exclude "transactional or relationship messages," which means, inter alia, any message "the primary purpose of which is . . . to facilitate, complete or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender [or] notification[s] 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 . . ."

Suppose, for example, that a law firm has ongoing relationships with clients and wants to tell them about a new service that the firm offers. Is an e-mail promoting that new service part of the existing relationship (thus not a commercial message), or does the new service mean a new relationship, so the e-mail is a commercial message subject to CAN-SPAM?

Does the answer to the foregoing depend on how closely the new service is related to existing services? Does it matter whether the new service involves any third parties in addition to the law firm and the client?

These are the types of questions that wenotify.net (www.wenotify.net), an Alameda company that sends move announcements and other communications on behalf of clients, asks every day.

Wenotify.net CEO Mike Levy says that "the burden [of complying with CAN-SPAM] is not so great." So if there is any doubt, Levy believes that the prudent approach is to assume that the message is commercial and comply fully with CAN-SPAM.

Levy's concern is that some recipients or ISPs may set their spam filters to routinely block commercial messages. In that case, the prudent approach could result in messages that are largely transactional or relationship in nature — and that the recipient likely would want or need to see — being characterized as commercial and, thus, not reaching the recipient.

By the end of 2004, the FTC must issue regulations on determining the primary purpose of an e-mail message. With a little luck, those regulations will substantially reduce uncertainty around the definition of commercial messages.

Results

So has CAN-SPAM made a significant contribution to reducing the amount of spam that e-mail users receive? It is difficult to find anyone who believes the answer is an unequivocal "yes."

Redwood City-based Postini provides e-mail security and management services for businesses. In an April 5, 2004, press release (www.postini.com/press/pr/pr040504.html), Postini reported that it found no reduction in spam for its 2,700 customers despite CAN-SPAM.

EDP Consulting Inc. in Oakland also conducted a spam study. Principal Jon Seidel analyzed e-mail that he received shortly after CAN-SPAM took effect (see www.edpci.com/Newsletter/NL7.html#1). He was able to achieve a quick reduction in spam by sending opt-out messages to two major spammers.

But Seidel points out two problems in relying on opt-out requests for anti-spam protection. "First . . . I had to spend a significant amount of time picking through the e-mails, doing the research . . . to identify potential unsubscribe candidates, and then trying it out . . . Second . . . I took a great risk: I confirmed my e-mail address to two spammers and could have received (might yet) much more spam."

Even Congress foresaw limited results from CAN-SPAM, predicting that "problems associated

with . . . unsolicited commercial electronic mail cannot be solved by federal legislation alone. [T]echnological approaches and . . . cooperative efforts with other countries will be necessary as well."

The future

CAN-SPAM required that the FTC submit a plan for a nationwide Do-Not-E-Mail registry no later than June 30, 2004. On June 15, however, the FTC told Congress that a Do-Not-E-mail registry would fail to reduce spam because there currently is no way to enforce the registry effectively.

By the end of 2005, the FTC must submit to Congress a report analyzing the effectiveness and enforcement of CAN-SPAM and recommendations, if any, for amending the act. The report must address relevant technological and marketplace developments; e-mail that originates in or is transmitted through other countries; and protection against obscene or pornographic e-mail.

The bottom line: Unless there is international cooperation and the right technological tools are developed, CAN-SPAM is a bit like a "No Trespassing" sign in the woods. People who are law-abiding likely will comply. Others likely will do whatever they want, figuring that the odds of being caught and punished are pretty remote.

• *Dana Shultz (www.danashultz.com) is a Bay Area licensing and intellectual property attorney.*