The CAN-SPAM Act Applies to Social Media Messaging, Rules Federal Court in California

by John L. Nicholson

On March 28, 2011, the U.S. District Court for the Northern District of California held in Facebook, Inc. v. MaxBounty, Inc.[1] *that messages sent by Facebook users to their Facebook friends' walls, news feeds or home pages are "electronic mail messages" under the CAN-SPAM Act. The court, in denying MaxBounty's motion to dismiss, rejected the argument that CAN-SPAM applies only to traditional e-mail messages. The ruling is the most expansive judicial interpretation to date of the types of messages falling within the purview of the CAN-SPAM Act. While the court did not address the underlying merits of the CAN-SPAM claims, companies using social media in marketing should verify that they (and any marketing services they engage) comply with CAN-SPAM's requirements for commercial messages sent via social media platforms.*

MaxBounty is an advertising and marketing company that uses a network of content-producing publishers to drive traffic to its customers' websites. MaxBounty acts as an intermediary between its network of publishers (advertisement content creators) and its customers (third-party advertisers).

In its complaint, Facebook alleged that MaxBounty engaged in a misleading and deceptive advertising scheme affecting Facebook users. According to the complaint, MaxBounty, through its network of affiliates, created fake Facebook pages that were intended to redirect Facebook users away from Facebook.com to third-party websites via a multi-step process:

- First, MaxBounty affiliates created numerous Facebook pages that functioned like (and, in effect, were) advertisements;
- Second, the Facebook pages displayed a message indicating that upon registration a user would be able to take advantage of a "limited time offer," such as receiving a gift card or becoming a product tester for a high-end product (e.g., an Apple iPad);

[1] *Facebook, Inc. v. MaxBounty, Inc.*, Case no. CV-10-4712-JF (ND CA)

- Third, the Facebook user was required to complete registration process that required the user: (a) to become a "fan" of the page, (b) to invite all of the user's Facebook "friends" to visit the page, and (c) to complete certain additional administrative registration requirements.

Once the user completed the registration requirements, he or she was directed to a third-party website to complete additional steps (e.g., signing up for numerous "sponsor offers" that were typically memberships to subscription-based services) in order to receive the item advertised on the Facebook page.

Facebook alleged that these actions constituted messages that violated the CAN-SPAM Act. The CAN-SPAM Act makes it "unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transaction or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading."[2] Under the act, an "electronic mail message" is defined as "a message that is sent to a unique electronic mail address,"[3] and an "electronic mail address" means a "destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the 'local part') and a reference to an Internet domain (commonly referred to as a 'domain part'), whether or not displayed, to which an electronic mail message can be sent or delivered."[4] MaxBounty challenged the characterization of the messages as "electronic mail" and, thus, the applicability of the CAN-SPAM Act.

Because the references to the "local part," the "domain part" and the other items are set off by commas, the court concluded that the only requirement for a message to be considered an "electronic mail message" under CAN-SPAM is a "destination . . . to which an electronic mail message can be sent." Accordingly, the court found that messages posted to another user's Facebook wall, news feeds or home pages are covered by the statute. The court also found it significant that the messages at issue involved "routing activity on the part of Facebook" and concluded that its interpretation was consistent with Congressional intent, which was to reduce the burden of misleading communications on the Internet.

The court relied primarily on two cases from the Central District of California involving MySpace: *MySpace Inc. v. The Globe.com, Inc.,*[5] and *MySpace Inc. v. Wallace.*[6] Both cases involved entities creating large numbers of MySpace profiles to send commercial and phishing "e-messages" to other MySpace users wholly within what is known as the "walled garden" of the MySpace service. In both cases, the court concluded that the e-messages at issue were "electronic mail messages" under CAN-SPAM.

In *MySpace v. The Globe.com*, the court found that the definition of "electronic mail message" was met because each user's messages resided at a unique URL and the Internet destination www.myspace.com. The court concluded that it was irrelevant that the messages were sent only within the "walled garden" of MySpace. The court in *MySpace v. Wallace* adopted the same reasoning, but went further in rejecting the defendant's arguments that to be "electronic mail messages" under the CAN-SPAM Act, messages must include a domain name and an external route for travel. The *MaxBounty* court held that the court in *Wallace* "reasonably concluded that Congress was aware of 'various forms of electronic communications when it drafted the [CAN-SPAM A]ct' and thus the plain language of 'electronic mails*[sic.]* address' includes alternate forms while also recognizing that the most commonly used form of electronic address was the traditional email with a local part and domain part (i.e. user@domain.com)."[7]

[2] 15 U.S.C § 7704(a)(1).
[3] Id. at § 7702(6)).
[4] Id. at § 7702(5).
[5] No. 06-3391 (C.D. Cal. 2007).
[6] 498 F. Supp. 2d 1293 (C.D. Cal. 2007).
[7] *MaxBounty* at 7, citing *Wallace*, 498 F.Supp.2d at 1300.

The *Facebook v. MaxBounty* court elected to adopt the definitional reasoning provided in *Wallace* and concluded that messages sent within Facebook using various Facebook messaging systems did constitute "electronic mail messages" for the purposes of the CAN-SPAM Act.

While technically the court's decision means that a message posted by one Facebook user to a friend's wall promoting the poster's home business could potentially be construed as a commercial "electronic mail message" under CAN-SPAM, it seems unlikely that Facebook or other social networking sites would sue their users under CAN-SPAM's private right of action for small numbers of such individual messages (or even large numbers, provided a business was not violating the site's terms of use).

However, the broad interpretation of the applicability of the CAN-SPAM Act could have far-reaching consequences for companies that use social media platforms for marketing. It is unlikely that more mainstream companies would adopt the aggressive tactics taken by MaxBounty, or that most social media platforms would take action against companies or users who were not abusing the system. Nevertheless, the CAN-SPAM Act requires that all commercial "electronic mail messages" comply with the following:

1. The header information for the message (including the "From," "To," "Reply-To," and routing information including the originating domain name and email address) must be accurate and identify the person or business who initiated the message;

2. The subject line must accurately reflect the content of the message;

3. The message must disclose clearly and conspicuously that it is an advertisement;

4. The message must include a valid physical postal address for the person or business who initiated the message;

5. The message must include a clear and conspicuous explanation of how the recipient can opt out of getting email in the future from the person or business who initiated the message;

6. Any opt-out mechanism must be able to process opt-out requests for at least 30 days after the message is sent. A recipient's opt-out request must be implemented within 10 business days.

The CAN-SPAM Act makes it clear that companies cannot contract away their legal responsibility to comply with the law. Both the company whose product is promoted in the message and the company that actually sends the message may be held legally responsible for compliance.

The FTC has been aggressive in pursuing violators of the CAN-SPAM Act's requirements, and those who use social media to send what have now been defined as "electronic mail messages" ignore the act's requirements at their peril.

If you have any questions about the content of this publication, please contact the Pillsbury attorney with whom you regularly work or the author below.

John L. Nicholson (bio)
Washington DC
+1.202.663.8269
john.nicholson@pillsburylaw.com