WSGR ALERT

APRIL 2011

FEDERAL COURT APPROVES THE APPLICATION OF THE CAN-SPAM ACT TO MESSAGES SENT WITHIN SOCIAL NETWORKING PLATFORMS

Ruling Carries Implications for Commercial Messaging on Social Networks

Several recent court decisions appear to expand the breadth of communications governed by the federal CAN-SPAM Act beyond traditional email.[1] Despite some defendants' vehement arguments in favor of limiting the scope of the CAN-SPAM Act solely to traditional forms of email, the federal district courts of California have applied the legislation to electronic messaging on social networking platforms such as Facebook and MySpace as well.

The most recent of these decisions, in *Facebook v. MaxBounty*,[2] held that the CAN-SPAM Act applied to commercial messages written on Facebook walls or in news feeds, inboxes, and user profiles. The decisions merit consideration by technology enterprises because social media platforms represent an increasingly critical channel for reaching consumers, and many investment opportunities depend in some measure upon in-platform or cross-platform messaging. Determining whether to contact consumers using social networks and how such messaging should occur in order to remain in compliance with the CAN-SPAM Act represents a growing concern as social media messaging continues to scale.

March 2011 Decision in *Facebook v. MaxBounty*

The *Facebook v. MaxBounty* case centered on MaxBounty's alleged practice of diverting Facebook users to third-party websites. Facebook claimed that MaxBounty induced Facebook users to engage in a protracted registration process in order to take advantage of illusory "limited time offer[s]" to test high-end electronics, such as the Apple iPad. The registration process required users to become a "fan" of the MaxBounty affiliate pages and invite all of their Facebook friends to do the same. Once the users completed this process, they were directed to a third-party website requiring additional registration steps, including signing up for paid subscription services. Facebook alleged that communications related to MaxBounty's traffic-generation scheme, which were made within the confines of the Facebook infrastructure, were subject to the requirements of the CAN-SPAM Act.

In its decision, the U.S. District Court for the Northern District of California relied on two cases from the U.S. District Court for the Central District of California for guidance in defining the scope of the CAN-SPAM Act. In *MySpace v. Wallace*[3] and *MySpace v. The Globe.com*,[4] the Central District considered MySpace's allegations that the defendants violated the provisions of the CAN-SPAM Act by engaging in a fraudulent scheme in which they used fake MySpace accounts to send unsolicited marketing messages to users' MySpace inboxes in attempts to induce users to disclose their MySpace login information (a scheme commonly known as "phishing"). The defendants argued that the CAN-SPAM Act should not apply to the communications at issue because, unlike traditional email, the messages remained within the MySpace platform, did not include simple mail transfer protocols, and had no domain name in the address. In each case, the court rejected the defendants' arguments and adopted an expansive view of the kinds of electronic messages falling within the purview of the CAN-SPAM Act. The courts held that messages sent within the MySpace platform required the use of an electronic routing system that necessarily implicated issues regarding volume of traffic and the utilization of infrastructure that Congress designed the CAN-SPAM Act to address.

---

[1] The Controlling the Assault of Nonsolicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) governs the transmission of "commercial electronic mail," which is statutorily defined as any electronic mail message that has the primary purpose of advertising or promoting commercial products or services, including content on a website operated for a commercial purpose. 15 U.S.C. 7701-13.

[2] *Facebook v. MaxBounty*, No. CV-10-4712-JF, 2011 WL 1120046 (N.D. Cal. Mar. 28, 2011).

[3] *MySpace, Inc. v. Wallace*, 498 F. Supp. 2d 1293 (C.D. Cal. 2007).

[4] *MySpace, Inc. v. The Globe.com, Inc.*, No. CV 06-3391-RGK (JCx), 2007 WL 1686966 (C.D. Cal. Feb. 27, 2007).

Continued on page 2...

Federal Court Approves the Application . . .

Continued from page 1...

Like the defendants in the *MySpace* cases, MaxBounty argued that the court should adopt a narrow view of the scope of the CAN-SPAM Act and exclude electronic communications on the Facebook system from its purview. The U.S. District Court for the Northern District of California rejected MaxBounty's argument and held that the CAN-SPAM Act applies to commercial electronic communications directed through routing activity to specific destinations. Therefore, the court held, commercial messages on or in Facebook walls, news feeds, message inboxes, and user profiles fall within the scope of the CAN-SPAM Act and its regulations.[5]

Implications for Companies and Consumers

Facebook v. MaxBounty, like the *MySpace* cases before it, demonstrates a trend toward broader application of CAN-SPAM Act restrictions. Companies would be prudent to analyze whether any commercial messages they send involve routing to a specific location within any electronic infrastructure, including a social networking service, because the *MaxBounty* and *MySpace* cases indicate that such messages implicate the requirements of the CAN-SPAM Act. Perhaps even more pragmatically, those who send—or benefit from—such messages may desire to take into account the rules and policies of the particular platform providers through which the messages are routed.

The CAN-SPAM Act provides private rights of action to those deemed to be providers of "Internet access service," as Facebook and MySpace were held to be in the *MaxBounty* and *MySpace* cases. Complying with the provider's rules and policies applicable to messaging on the platform may, as a practical matter, decrease the likelihood of a platform provider bringing a private action under the CAN-SPAM Act against a company for its messaging on the platform.

To the extent that the CAN-SPAM Act applies to in-platform messaging, familiarity with the basic requirements of the act may be helpful.

The Requirements of the CAN-SPAM Act of 2003

Among other things, the CAN-SPAM Act provides that it is unlawful for any person to initiate the transmission of a commercial electronic mail message that:

- **Contains header information that is materially false or misleading.** Header information includes the "From," "To," "Reply-to," and routing information for the message. In general, header information is materially misleading if the sender obtained the originating mail address, domain name, or Internet Protocol address of the message through fraud, or if the header information fails to accurately identify a computer used to initiate a message because the sender knowingly uses another computer to relay or retransmit the message to disguise its origin.

- **Contains a deceptive subject line.** The message's subject line must accurately reflect the contents of the message.

- **Does not contain a functioning return email address with notice that the receiver can request to opt out from future messages.** The message should include a clear and conspicuous explanation of how the recipient may opt out of future messages, and the opt-out mechanism must function for at least 30 days after the message is sent. The sender must process all opt-out requests within 10 business days of receipt.

- **Does not contain a valid postal address of the sender and clear and conspicuous identification that the message is an advertisement or solicitation.** The recipient of a commercial electronic message must be able to identify the nature of the message, as well as a valid brick-and-mortar postal address for the sender.

The CAN-SPAM Act further prohibits the use of automated programs (i.e., "bots" or "scripts") to register for multiple email or online user accounts, or to generate commercial emails for random recipients.

The Federal Trade Commission also has adopted several rules implementing the CAN-SPAM Act. These rules cover matters such as the definition of a "commercial" email message and the requirements that apply when a message advertises or promotes the products or services of more than one entity.

For more information, please visit http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/clientalert_canspam.htm to read our previous WSGR Alert on the CAN-SPAM Act.

Application to Wireless Communications

Because social media platforms often are accessed via mobile devices, the federal regulations governing commercial communications to wireless devices also may be implicated. The Federal Communications Commission (FCC) has adopted specific wireless CAN-SPAM Act regulations that require senders to obtain express prior authorization before transmitting commercial email messages to Internet domains assigned by wireless providers for use on mobile devices.[6]

---

[5] The court went on to dismiss Facebook's additional claims against MaxBounty for fraud, aiding and abetting fraud, and conspiracy. As of April 18, 2011, there have been no further filings in the case.

[6] 47 C.F.R. § 64.3100.

Continued on page 3...

Federal Court Approves the Application. . .

Continued from page 2...

These wireless CAN-SPAM Act rules operate in concert with separate FCC commercial text message rules implementing the Telephone Consumer Protection Act of 1991 (TCPA). Among other things, these rules prohibit any text messages sent using an "automated dialer system" (which may include a computer) without obtaining the recipient's prior express consent.[7] The increasing popularity of group text and related services, as well as the scaling of such services, likely will increase the need for familiarity with these rules by many companies, especially those seeking to use them for commercial messaging.

To avoid potential civil and criminal liability, any sender of electronic messages on social media platforms should keep in mind that any commercial messaging likely implicates the requirements of the TCPA. Commercial messaging sent using social networking functionality also may implicate other laws and regulations, including those applicable to text messages. Companies should understand the laws and regulations applicable to commercial communications prior to engaging in promotional campaigns using social networks and other online services.

Navigating the Broadened CAN-SPAM Landscape

Wilson Sonsini Goodrich & Rosati's attorneys routinely counsel clients on compliance with the CAN-SPAM Act, other laws applicable to commercial messaging, and related marketing and privacy issues. Additionally, the firm has played a leading role in litigation and regulatory efforts concerning online marketing and privacy. If you have questions regarding any of these areas, please contact Tonia Klausner at tklausner@wsgr.com or (212) 497-7706; Gerry Stegmaier at gstegmaier@wsgr.com or (202) 973-8809; Matt Staples at mstaples@wsgr.com or (206) 883-2583; or your primary contact at the firm.

---

[7] 47 C.F.R. § 64.1200.

WSGR

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

This WSGR Alert was sent to our clients and interested parties via email on April 19, 2011. To receive future WSGR Alerts and newsletters via email, please contact Marketing at wsgr_resource@wsgr.com and ask to be added to our mailing list.

650 Page Mill Road
Palo Alto, CA 94304-1050
Tel: (650) 493-9300 Fax: (650) 493-6811
email: wsgr_resource@wsgr.com

www.wsgr.com