

Privacy Issues for Mobile Devices

Liisa M. Thomas

WINSTON
& STRAWN
LLP

Mobile devices raise a new and complex set of concerns for companies that are trying to manage compliance with privacy laws. While there are several laws that cover how companies can contact consumers on a mobile device—the Telephone Consumer Protection Act (“TCPA”), the CAN-SPAM Act, as well as Section 5 of the Federal Trade Commission Act, often referred to as the Deceptive Trade Practices Act (“DTPA”) and similar state laws—none provide easy answers, nor do they provide answers for all situations in which a consumer may be contacted. What should a company do? The baseline is to start with the deceptive trade practices laws, then look to the specifics of laws such as CAN-SPAM and TCPA. In addition, industry guidelines can also provide assistance, especially when trying to determine what might be viewed as a deceptive or unfair practice.

AVOID “DECEPTION” AND “UNFAIRNESS” ALLEGATIONS

The DTPA prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce. Under its authority from the DTPA, the Federal Trade Commission (“FTC”) has actively pursued companies that either engage in “deception” by violating their stated privacy practices, or those that engage in “unfair” acts by failing to protect personally identifiable information. Similar state laws are used by state attorneys general (“AGs”), and some of those state laws have private rights of action. When looking at mobile privacy issues, the DTPA could be used against a company that fails to use information as it describes to consumers.

For example, take a company that runs a text-based sweep-stakes entry program, in which a consumer texts “ENTER ME” to enter the sweepstakes. In ads encouraging people to enter, the company promises, “We will only use your information to enter you in this program and to send you an announcement if you win.” If the company then adds the person to a marketing database, and sends that person marketing messages, the company may find itself in a battle with the FTC or a state AG, fighting allegations that it has engaged in a deceptive act. Thus, when determining from a privacy standpoint whether to contact a consumer on his or her cell phone, the company should look at the representations that it has made about how information will be used. Violating those representations might result in a violation of the DTPA.

In addition to looking at a company’s own statements, it is also helpful to look at the industry standard, often expressed in self-regulatory programs. For mobile marketing, one such program, the widely recognized Mobile Marketing Association, has issued a set of guidelines outlining for its

members what they should or should not do when marketing to consumers on their cell phones. Included in the guidelines are a requirement that consumers be provided with notice regarding how their numbers will be used, and that they opt-in to such use before the numbers are used. The guides anticipate that consent might be provided by text message from the consumer to the company or through an online registration process, among other possibilities. The guides specify that when consent is obtained, that consent should be treated as consent for a particular program, not for all communications generally. The guides also require a simple process for consumers to opt out of receiving future marketing texts, that the messages are appropriately targeted to their audience, and that companies send a limited number of text messages.

TAKE CARE IF USING AN AUTO-DIALER

Certain requirements apply to use of consumer's cell phone numbers if they are going to be contacted using auto-dial technology. In particular, under the TCPA, companies are prohibited from making any calls using an automatic tele-phone dialing system unless the recipient has given his or her prior express consent. The Federal Communications Commission ("FCC") has stated that "calls" in this context include both voice calls and text messages. The question, of course, is what constitutes an auto-dialer, and how do you know that it has been used? This issue was examined in *Satterfield v. Simon & Schuster*, where in June 2007 the Northern District of California held that the TCPA did not apply to a text message campaign because the system used was not an "automatic dialing system," inasmuch as the system sent messages to a targeted promotional list of numbers and did not randomly or sequentially generate calls. That decision was subsequently overturned, however, with the Ninth Circuit holding in July of this year that the critical issue was not whether the system did or did not randomly store and call numbers, but instead whether it had the ability to do so. If it did, then it was an auto-dial system, and as such, TCPA restrictions on such a system would apply.

Other cases, interestingly, have not analyzed this issue, but instead have simply presumed that if there is a text message being sent, it is being sent through auto-dial technology. For example, in September 2008, the Timberland Company and its mobile marketing vendor, GSI Commerce, Inc., were alleged to have sent thousands of unsolicited text messages to consumers to market upcoming sales, in violation of the TCPA. As part of the settlement agreement, Timberland and GSI Commerce agreed to pay \$7 million and follow best practices for marketing in the future. In 2007, a similar settlement was reached in a class action brought against Distributive Networks LLC. Distributive Networks, a wireless content and technology company, was sued by a class of approximately 1,000 consumers who allegedly received unwanted text messages encouraging the consumers to subscribe to Distributive's services. Distributive agreed to settle and, as part of the settlement, to pay \$150,000. This amount included a \$150 payment to each member of the class. While Distributive did not admit fault, it did indicate that two of its affiliates, as well as the carriers that were sending the messages for Distributive, were abusing Distributive's text message rules.

ALSO TAKE CARE IF SENDING ADVERTISING CONTENT IN A MESSAGE

Under the TCPA, regardless of whether an auto-dialer is used, companies are prohibited from initiating a telephone solicitation—i.e., a call made for the purpose of encouraging the purchase of goods or services—to a number listed on the do-not-call registry without either having (1) the

recipient's prior express invitation or (2) an established business relationship with the recipient. In addition, a company cannot send a telemarketing message (a message to encourage the purchase of a product or service) if it does not have in place measures for creating its own opt-out list. (Of course, if an auto-dialer is used, then the company will be required to obtain consent to send the message, and will as a result fall into the first exception.)

If the text message contains a solicitation, other parts of TCPA must be followed. In particular, the company (1) may send the message only between 8 a.m. and 9 p.m. and (2) must maintain a process for obtaining and recording any opt-out requests it receives.

SENDING TEXT ADS THAT "REFERENCE" A DOMAIN NAME

In addition to TCPA requirements, there are certain re-quirements for sending text messages under CAN-SPAM, the law more familiar to most as having restrictions in place for sending commercial email messages. Under CAN-SPAM, companies must take certain steps if sending "mobile service commercial messages;" in other words, if sending text messages through technology known as "referencing" a domain name. What does this mean? It refers to messages that are sent to a consumer's cell phone through the mobile service provider's email gateway (i.e., behind the scenes, the message is being sent to 5555555555@wirelesscarrier.com). Whether a message references a domain is not apparent to the consumer, and thus each time a company considers what law applies to the sending of text messages, it must work with its technical team to determine whether the message is being sent through the email gateway (referencing a domain name).

If CAN-SPAM applies, companies are prohibited from sending "mobile service commercial messages" unless the subscriber has provided "express prior authorization." Express consent can be given in writing or verbally. If in writing, the consent must include a signature or digital equivalent. The signature, if in digital form, need only be a record that the consumer consented to receive the message. Consent is generally viewed to be limited to that for which it was obtained. For example, a consumer who authorizes a car repair company to send her a notice when the car repairs are complete has not provided blanket authorization to receive text ads from the company. Similarly, if authorized by a consumer to send text ads about the company, the company is not then authorized to send ads for a third party.

Once consent has been obtained, when sending a text message ad, the company must identify itself in the text message, include in each message a free electronic mechanism (a free text number to dial, for example) for consumers to opt out, and ensure that the opt-out mechanism functions for 30 days after the message is sent. In its comments, the FCC clarified that a company can continue to send messages to the consumer until the consumer revokes his or her authorization. If consent is revoked, the company must stop sending text messages to the consumer within 10 days.

The above-described restrictions and requirements do not apply if the message is "transactional" in nature, including those that "facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into." For example, delivering a coupon that a consumer has requested might be viewed as transactional. Transactional messages are also those that "deliver

goods or services . . . that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the seller.” Thus, a message with a flight alert that the consumer has requested might also be viewed as transactional.

CONCLUSION

Any company contemplating communicating with consumers on their mobile devices should use caution. There are many specific laws that apply to such activities, as well as potential for liability under deceptive trade practices laws. In general, if a company has obtained a consumer’s consent to send the communication, it will have gone a long way toward addressing compliance concerns with these laws.

Liisa M. Thomas is a partner in the advertising law department at Winston & Strawn LLP and spearheads the firm’s privacy law initiative. Ms. Thomas, who focuses her practice on interactive advertising law issues, may be reached at lmthomas@winston.com. The information contained in this article is not intended as, nor should it serve as a substitute for, legal advice, which turns on specific facts.

This information or any portion thereof may not be copied or disseminated in any form or by any means or downloaded or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

Charlotte Chicago Geneva Hong Kong London Los Angeles
Moscow New York Newark Paris San Francisco Washington, D.C.

www.winston.com

WINSTON
& STRAWN
LLP