PUT DOWN YOUR PHONE AND WATCH THOSE TEXTS

New Regulations Impacting Your Outreach to Customers, Clients and Contacts

Molly A. Arranz Amundsen Davis LLC

The speed, sophistication, and ease of a company's communications or outreach with and to their customers or clients only continues to get better and better. Just ask your marketing and sales teams about the new technology or platforms at their disposal to send out promotions, discounts, reminders, and hot deals. Plus, sharing of consumer data with trusted business partners is commonplace, all in an effort to promote growth of company revenue and spreading a company's brand.

At the same time, every company knows (or should know) about the importance of getting the right permission or consent before sending those promotions or reminders and before sending a "lead" to a business partner for their outreach or touchpoint. Each should know how to offer consumers an opportunity to be forgotten or to not receive promotions or communications anymore. To date, federal statutes, like the Telephone Consumer Protection Act (TCPA), and regulations put in place by the Federal Communications Commission (FCC), have guided companies in various industries on what level of consent is necessary before sending SMS texts or making phone calls and what's required for giving the recipient an opportunity to revoke consent. The particulars for these marketing or sales activities have been fairly well established.

However, reevaluation of these guardrails should be considered given two recently released Reports and Orders by the FCC. They are set to have a significant impact on what permissions you may need in place before sending SMS texts or making phone calls, what options you need to make available for opting-out of subsequent texting or phone calls—and how you respond to those opt-outs.

ONE-TO-ONE CONSENT FOR LEAD-GENERATED TEXTS

Companies and consumers can both agree that text messaging is invaluable "to stay in touch with friends and family" and "to do business"—that text messaging is "an expected trusted source of communications" and shouldn't be used as an annoyance or scam.

These values have been reiterated by the FCC in a Second Report and Order released on December 18, 2023. The 72-page Order makes clear that the Commission remains vigilant against a "rise of junk texts" that jeopardize consumer trust. At the same time, in that Order, the FCC proposes closing a "Lead Generator Loophole." This proposed change could dramatically affect companies in many industries that rely upon their business partners to obtain the right permissions or consent to send texts and make calls to customers.

Take, for instance, a company that provides certain products or services, such as loans and related offerings. It may rely upon business partners to find potentially interested customers, to gather their contact information, and then to share this information so the company can reach out to the customer and promote the requested services or products. This sort of "leads-generation" oftentimes plays out with the company's sales team sending multiple text messages or calls to those interested prospects. Before that point, a business partner makes a disclosure and provides an opt-in to calls and texts from "business partners."

In the December 2023 Report and Order, the FCC reiterates that texters and callers must obtain prior express written consent before making the call or sending the text but now, also finds that this consent will only apply to a single seller at a time. The FCC has proposed this revised rule, explaining companies need to comply with a "one-to-one consent" rule. The Rule, not yet in effect, would mean that group consent is insufficient; a consumer, on an individual basis, must convey consent to a company for the calls or text messages about the products or services.

The FCC also adopted two other pro-

tections for the one-to-one consent: that consent only comes after a clear and conspicuous disclosure that the consumer will get those texts and calls; and, if consent is obtained on a comparison shopping website, the texts or calls that follow must be "logically and topically" related to the website offering. Practically speaking, for both of these requirements, compliance may be a challenge. The FCC provides a nebulous standard for "clear and conspicuous"—i.e., what would be apparent to the reasonable consumer—and for companies to determine what is logically and topically related will require them to only send texts or make calls limited to content consumers "would clearly expect."

With this, there appears to be an imminent sunset on entities relying on "bundled consent" for contacting customers and consumers. Though the Order notes the implications of requiring one-to-one consent and has sought comment on ways to "refine our one-to-one consent rule to further mitigate any burdens it may create for businesses," change is coming.

The December 2023 FCC Order notes that amendments may occur and allows businesses a 12-month safe harbor to ensure compliance. The effective date will be announced by subsequent Public Notice.

"EASING" REVOCATION OF THE CONSENT TO BE TEXTED OR CALLED

The FCC kept rolling out additional rules on texting and calling. On February 16, 2024, it released a Report and Order and Further Notice of Proposed Rulemaking meant to address consumers' "right to revoke" consent after deciding they no longer want robocalls or robotexts. The Order was meant to establish new consent protections and to "strengthen consumers' ability to revoke consent so that it is simple and easy."

However, when taking a deeper dive into the particulars, companies, especially those in certain industries, may find more head-scratching than clarity.

Specifically, this Order appears to target texts and calls promoting consumer goods and services and transactional texts those companies may send. The Commission noted that these robocalls and robotexts are restricted by prior express consent. In the February Order, the FCC explained that, going forward, revocation of consent for calls and texts can be made in any reasonable manner. This means that when a consumer replies to a text, for instance, and uses the words "stop," "quit," "end," "revoke," "opt-out," "cancel," or "unsubscribe," this is a per se reasonable means to revoke consent. This is certainly a new rule that all companies need to review.

However, the Order also noted that there are some text messages and phone calls that are exempt from the consent requirement, such as certain health care related or bank fraud communications. And the Order includes proposed rulemaking on revocation that could affect these exempt messages. These types of messages include, for instance, "health care" messages made by a covered entity or business associate, as defined in the HIPAA Privacy Rule, and messages from financial institutions regarding transactions that may involve fraud or identity theft or to notify a consumer about possible breaches of personal security. As long as the company (the health care provider or bank) follows other conditions on the number and frequency of messaging, consent is not required and a request to stop receiving these messages required very specific protocols such as texting "STOP."

The FCC makes clear that the new rule establishes that consumers or recipients can opt-out of or revoke consent for future messages in any reasonable manner and explains this only applies to the calls and texts for which a company had to obtain consent, for instance, marketing and transactional texts and calls. The Order provides that even when that consent has been revoked, the same company can still send exempted messages.

However, the FCC goes on to recognize that consumers may inadvertently opt out of exempted informational calls or messages such as fraud alerts when attempting to stop unwanted telemarketing calls from that same company. The Commission also explained that if a revocation request is made directly in response to an exempted informational call or text, this would mean an opt-out of all further non-emergency calls and texts. No exempt or non-exempt messages, period. The "consumer's intent" is to no longer receive such exempted informational calls from the caller and also "all calls from the caller."

Practically speaking, these proclamations present some challenges. Consider the following. What if a person texts back "STOP" in response to a bank's text message regarding financial safeguards being offered to protect against identity theft? Unless you get better information from the consumer—you can send one clarifying text to see if the recipient wanted to stop receiving all texts—the bank needs to stop sending all non-exempt robocalls and robotexts to that person. This assumes the text does not qualify or could not be construed as an exempt text.

If, however, a person texts back "STOP" to a bank's text message about a potential breach of that person's security, all exempt and non-exempt messages, be it by phone or text, must stop. Again, there is the opportunity to get clarity on the extent of revocation, as well, but stopping all contact can be an administrative challenge, to say the least.

This FCC Order also addresses the timeframe for honoring a do-not call or revocation request and seeks comment on application to wireless providers and the "Wireless Provider Exemption."

These proposed rules remain open to comment; however, certain new requirements on company protocol on "scrubbing" or deleting customer, client or even patient data appears unavoidable.

WHAT THIS MEANS FOR YOUR BUSINESS

There is added pressure on many companies to expand their business and invest in new sales and marketing opportunities. Companies are regularly being presented with improved technologies that allow them to reach customers and clients faster and seamlessly.

Undoubtedly, businesses have in place appropriate practices and protocols to get the right level of permission and to instill the appropriate level of training to not only comply with existing legal restraints but to refrain from sending annoying texts or making bothersome calls.

Now, with these new rules on the horizon, a refresh or revision of these consumer and customer disclosures and a reevaluation of the policies and protocols is critical. Start with a regrouping with your employees that take lead on sales and marketing to ensure you know how and when they communicate with your clients and customers. Evaluate what your business partners are doing on your behalf. With the safe harbor in place for compliance, now is the time to get this in order. The downside to not doing so could be dramatic given the statutory fines baked into the TCPA and related statutes.

Molly Arranz is the chair of Amundsen Davis's Cybersecurity & Data Privacy Service Group. She is a certified privacy professional (CIPP-US) and a recognized Privacy Law Specialist by the American Bar Association. Contact: marranz@amundsendavislaw.com