

FCC Publishes Robotexting Report and Order and FNPRM in the Federal Register

April 11, 2023

On April 11, 2023, the Federal Communications Commission (FCC or Commission) published a Report and Order (R&O) in the Federal Register, setting an effective date of May 11, 2023 for certain of its rules. The R&O establishes mandatory text blocking obligations for mobile wireless providers, and builds on the Commission's previous Notice of Proposed Rulemaking (NPRM). The Commission also published a Further Notice of Proposed Rulemaking (FNPRM) seeking comment on establishing additional robotexting rules in the Federal Register on April 7. Accordingly, comments on the FNPRM are due on May 8, and reply comments are due June 6.

Below, we provide a high-level summary of the R&O and FNPRM.

For the first time, the Commission adopts mandatory text blocking requirements for mobile wireless providers.

Mandatory Blocking. The R&O requires mobile wireless providers to block certain robotexts that are highly likely to be illegal. Specifically, the R&O requires mobile wireless providers to block—at the network level—texts purporting to be from North American Numbering Plan (NANP) numbers on a reasonable Do-Not-Originate (DNO) list, which includes numbers that purport to be from invalid, unallocated, or unused numbers, and NANP numbers for which the subscriber to the number has requested that texts purporting to originate from that number be blocked. The R&O explains that the Commission's decision to require blocking rather than relying on industry's voluntary efforts to block is due to "the heightened risk of text messages as both annoyance and vehicles for fraud." The R&O's requirement to block texts that purport to be from numbers on a reasonable DNO list does not include text messages from short codes.

Authors

Kevin G. Rupy
Partner
202.719.4510
krupy@wiley.law
Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law
Stephen J. Conley
Associate
202.719.4572
sconley@wiley.law
Kelly Laughlin
Associate
202.719.4666
klaughlin@wiley.law

Practice Areas

Communications Enforcement & Compliance
Telecom, Media & Technology

Point of Contact. The R&O also requires mobile providers to ensure that senders have access to points of contact to report erroneously blocked texts, similar to the Commission's previous work to mitigate the risk of erroneous call blocking. The R&O only requires providers to accept blocking complaints from senders that can provide documented, objective evidence of blocking. Additionally, the R&O gives providers flexibility to establish their own point of contact or to require their aggregator partners and blocking contractors to establish a point of contact. The Commission declines to set time limits on resolving complaints of text blocking errors.

Compliance Deadline. While the R&O will take effect on May 11, mobile wireless providers will not be required to comply with the new rules until six months after the Commission publishes notice of the Office of Management and Budget's approval of the R&O under the Paperwork Reduction Act. Publication of this notice may take several weeks or even months.

Legal Authority. In the R&O, the Commission concluded that it has legal authority to require providers to block certain text messages originating from NANP numbers and to require blockers to establish a point of contact for receiving and resolving blocking complaints through the Telephone Consumer Protection Act (TCPA), Truth in Caller ID Act, and Title III of the Communications Act (the Act). The TCPA restricts certain autodialed and prerecorded or artificial voice calls to residential and wireless telephone numbers, absent the prior express consent of the called party. The R&O explains that texts are included in the term "call" for purposes of the TCPA, giving the Commission authority to regulate certain text messages under the TCPA—especially with regard to messages sent using an autodialer and without consent of the called party.

The Truth in Caller ID Act makes unlawful the spoofing of caller ID information "in connection with any voice service or text messaging service . . . with the intent to defraud, cause harm, or wrongfully obtain anything of value." The R&O states that this provides the Commission with authority to adopt a blocking requirement for calls that unlawfully spoof numbers on reasonable DNO lists.

Lastly, the R&O explains the Commission has authority to adopt text blocking rules under Title III of the Act because Title III "endow[s] the Commission with 'expansive powers' and a comprehensive mandate to 'encourage the larger and more effective use of radio in the public interest.'" The R&O finds that "the requirements we adopt for mobile wireless providers here are necessary to protect the public from illegal text messages and that such a requirement is in the public interest."

Other Proposals. The R&O declines to adopt rules for several of the other topics covered in the initial NPRM. The R&O declines to adopt text blocking notifications, rules on safeguarding against blocking of texts to 911 and other emergency numbers, and standards to ensure competitively neutral and content-neutral grounds for blocking. Lastly, the R&O declines to adopt caller ID authentication requirements for text messages because the record reflected uncertainty about the current feasibility of such a requirement.

The FNPRM seeks comment on additional protections for consumers against illegal robotexts.

The FNPRM seeks comment on four broad questions:

- Whether to require terminating mobile wireless providers to block text messages when notified by the Commission that they are likely scams;
- Whether to mandate text message authentication;
- Whether to extend Do-Not-Call (“DNC”) protections to marketing text messages; and
- Whether to ban the practice of obtaining a single consumer consent as justification for calls and texts from multiple—sometimes hundreds—of sellers and potential fraudsters.

Blocking Texts Upon Commission Notification. The FNPRM proposes to require terminating mobile wireless providers to investigate and potentially block texts from a sender after they are on notice from the Commission that the sender is transmitting suspected illegal texts—similar to the requirement for gateway providers with respect to voice calls. The FNPRM asks whether there are differences between calling and texting that would suggest this model would not work well for texting, and what the cost to providers would be for implementing such a requirement.

Text message authentication. As the R&O declined to adopt caller ID authentication requirements for text messages based on the current record, the FNPRM seeks comment on the prevalence of number spoofing and if there are other solutions that are better targeted to address the problem of spoofed text messages. The FNPRM asks whether a specific set of providers is responsive for spoofed text messages, similar to the dynamic at play in the robocalling context.

Extending DNC Protections to Text Messages. The FNPRM proposes to clarify that National DNC Registry Protections apply to text messages as well as voice calls and codify this clarification in the Commission’s rules. The FNPRM explains that the Commission has stated “text messages” are “calls” for purposes of the TCPA, but has not explicitly included text messages in the codified DNC rules. The Commission’s DNC rules protect wireless phone subscribers by requiring prior express invitation or permission in writing for calls to wireless numbers on the DNC Registry. The FNPRM asks whether codifying the DNC protections to marketing text messages specifically would further protect consumers from unwanted marketing text messages.

Closing the Lead Generator Loophole. The FNPRM proposes to ban the practice of obtaining a single consumer consent as grounds for delivering calls and text messages from multiple marketers on subjects beyond the scope of the original consent. The FNPRM explains that lead generators and data brokers may use hyperlinked lists to harvest consumer telephone numbers and consent agreements on a website and pass that information to telemarketers and scam callers. The Commission asks whether to amend its TCPA consent requirements to mandate that consent be considered granted only to callers “logically and topically” associated with the website that solicits consent and whose names are “clearly disclosed” on the same webpage.

Legal Authority. Lastly, the FNPRM seeks comment on the Commission’s authority to adopt each of the measures proposed in the FNPRM. Specifically, the FNPRM asks whether the Commission has legal authority to adopt the proposed rules under the TCPA, TRACED Act, Truth in Caller ID Act, and/or section 251(e) of the

Act. The Commission notes it found authority to mandate STIR/SHAKEN implementation based on section 251 (e) of the Act because it was “necessary to enable voice service providers to help prevent these unlawful acts and to protect voice service subscribers from scammers and bad actors.” The FNPRM indicates that the Commission believes the same reasoning applies here given Congress’s focus on text messages and seeks comment on that conclusion.

The new rules may have a broad impact across the telecommunications space for voice service providers who provide text messaging services, but also for enterprises engaged in marketing via text and other providers of ancillary services.

We have a deep and experienced robocalling and robotexting bench. Our experts handle federal and state policy issues, compliance with federal and state requirements, and complex TCPA issues. For more information about the FCC’s new item, please contact one of the authors listed on this alert.