

FCC Seeks Comment on Proposed Rules for Blocking Illegal Robotexts

September 29, 2022

On September 27, 2022, the Federal Communications Commission (FCC or Commission) released a Notice of Proposed Rulemaking (NPRM) seeking comment on a proposal that would require mobile wireless providers to block illegal text messages and applying caller ID authentication standards to text messaging. To date, the FCC's efforts have largely focused on robocalls, not robotexts. Accordingly, this NPRM represents a significant new undertaking by the FCC. These efforts – if adopted – will have a wide impact across the wireless messaging ecosystem.

Below, we provide background and a high-level summary of the new NPRM. Comments are due 30 days after the NPRM is published in the Federal Register, and replies will be due 45 days after the NPRM is published in the Federal Register.

The FCC Notes an Increase in Illegal and Unwanted Text Messages as the Premise for Its New NPRM

As a basis for the proposed rules, the NPRM notes that consumers are receiving increasing numbers of illegal and unwanted text messages, with the Commission reporting that it received approximately 14,000 consumer complaints about unwanted text messages in 2020, representing a 146 percent increase in the number of complaints from the year before. The Commission has subsequently received 15,300 consumer complaints about unwanted texts in 2021, and 8,500 such complaints through June 30, 2022.

The NPRM also notes that text message-based scams can harm consumers by including links to phishing websites and loading unwanted software onto a device. It further states that, like robocalls,

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

The Telephone Consumer Protection Act (TCPA)

scam texts can involve falsifying caller ID information that appears on the texted party's phone with the intent to defraud or wrongfully obtain something of value. According to the NPRM, scammers stole over \$86 million through spam texting fraud schemes in 2020.

Finally, the NPRM notes that the "ubiquitous" use of text messaging services by consumers also exacerbates the risk of robotexts. The NPRM cites to industry data indicating that consumers read nearly all texts they receive, open a far larger percentage of text messages compared to email, and open text messages far more quickly than email.

The Legal Landscape for SMS Messages Is Distinct from Robocalls

The NPRM also provides an overview of the regulatory framework currently applicable to text messaging services, which in many respects is distinct from the legal and regulatory landscape for robocalls. In particular, the NPRM discussed the following frameworks and how they apply to text messaging:

- *Telephone Consumer Protection Act (TCPA)*. The NPRM explains that the TCPA generally requires callers to receive consumer consent before making calls using an automated telephone dialing system or an artificial voice. The Commission has applied the consent requirement to text messages using an autodialer and clarified that the TCPA also covers internet-to-phone text messages sent to a carrier's server and then routed to a consumer's phone.
- *National Do-Not-Call Registry (DNC)*. The NPRM also points to the DNC, noting that it protects consumers from unwanted text messages containing marketing when the consumer has placed their number on the registry.
- *Truth in Caller ID Act of 2009*. The Truth in Caller ID Act of 2009 prohibits caller ID spoofing if the goal is to defraud, gain something of value, or otherwise cause harm. As detailed in the NPRM, the Commission has updated its Truth in Caller ID rules to encompass text messages.
- *STIR/SHAKEN*. The NPRM also discussed the STIR/SHAKEN framework, which is a caller ID authentication standard that helps to combat illegal caller ID spoofing and allows voice service providers to verify that the caller ID information accompanying a call matches a number the caller is authorized to use. The STIR/SHAKEN framework was developed for internet protocol networks to authenticate caller ID information. The FCC recognizes that STIR/SHAKEN standards do not currently support text messages, but work on such standards is ongoing.
- *Call Blocking*. Finally, the NPRM discusses the current call blocking approach, explaining that the Commission has permitted voice service providers to block unwanted and illegal phone calls, in addition to continuing to pursue enforcement actions against illegal robocallers. These call blocking practices currently do not apply to text messages.

The NPRM Seeks Comment on Applying Call Blocking and STIR/SHAKEN Frameworks to Texting

In the NPRM, the Commission proposes to protect consumers from the increasing number of illegal text messages by extending some of the consumer protections against illegal robocalls to text messages. Specifically, the Commission seeks comment in two key areas: (1) whether to permit the mandatory blocking of illegal texts; and (2) whether to require providers to implement caller ID authentication for text messages. Importantly, the NPRM also asks questions about the Commission's legal authority to adopt such measures.

Mandatory Blocking of Illegal Texts. The Commission proposes to require mobile wireless providers to block text messages that appear to be from invalid, unallocated, or unused numbers, and numbers on the "Do-Not-Originate" (DNO) list at the network level, without consumer opt-in or opt-out. The Commission seeks comment on this proposal and whether the Commission should adopt the same "highly likely to be illegal" standard for unwanted text messages that the Commission adopted for call blocking.

The Commission also seeks comment on the need for mandatory blocking and on the current landscape surrounding robotexts. Among other questions, the NPRM seeks comment on:

- Whether text messages from invalid, unallocated, or unused numbers, and numbers on the DNO list, represent a material fraction of unwanted text messages;
- Whether numbers placed on the DNO list are used for illegal texts;
- The extent to which spoofing is a problem with regard to text messaging;
- What voluntary text blocking providers are currently doing to protect their subscribers;
- Whether device-level or application-based text blocking is effective to reduce illegal texts;
- How to protect consumers from erroneous blocking of emergency text messages; and
- Whether the Commission should apply any safeguards for text blocking requirements to mitigate erroneous blocking.

Applying Caller ID Authentication Requirements to Text Messages. The Commission also tentatively concludes that providers should implement caller ID authentication for text messages. The NPRM also seeks comment on the progress of efforts to extend authentication to text messages and asks whether the current STIR/SHAKEN governance system can accommodate authentication for text messages with modification, or whether a new governance system is required.

If the Commission concludes that providers should implement caller ID authentication for texts, the NPRM seeks comment on what timeline it should establish for adoption. The NPRM asks whether the scope of any required implementation should be limited to voice service providers who are subject to the STIR/SHAKEN implementation mandate and provide text message services, or whether the Commission should define a new class of providers subject to authentication requirements for text messages.

The NPRM also requests comment on whether to require providers with non-IP network technology to develop a non-IP solution to enable the authentication for text messages, whether to prohibit providers from imposing additional line-item charges for authentication of text messages, and on other actions the Commission could take to address illegal text messages.

Legal Authority. Finally, the Commission solicits input on whether it has authority to adopt the NPRM's proposed rules under Section 251(e) of the Communications Act (the Act), which gives the Commission "exclusive jurisdiction over those portions of the North American Numbering Plan that pertain to the United States." The Commission previously determined that Section 251(e) gave the Commission authority to implement STIR/SHAKEN for voice service providers and engage in call blocking to prevent the fraudulent exploitation of numbering resources. The Commission asks whether this authority extends to text messages.

Alternatively, the Commission seeks comment on whether it has statutory authority to mandate that providers implement authentication for text messages under the TRACED Act, the TCPA, or the Truth in Caller ID Act. Lastly, the Commission seeks comment on the scope of its authority under Title III of the Act to adopt the proposed rules as Title III provisions give the Commission authority to establish license conditions in the public interest.

The NPRM's possible impact on the regulatory landscape for mobile wireless providers is broad. The FCC and Federal Trade Commission (FTC) have been expanding their oversight and broadening regulatory obligations across this sector. The proposed rules may impact voice service providers who provide text messaging services, but also intermediate providers, gateway providers, 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 NPRM, please contact one of the authors listed on this alert.

Kelly Laughlin, a Law Clerk at Wiley Rein LLP, contributed to this alert.