



CIVIL

Safeguarding Consumer Communication: Addressing Unsolicited Commercial Communication

AUTHOR Aardra S Prathap

PUBLISHED 6 June 2025

Introduction

Unsolicited Commercial Communication, often referred to as spam, has become a significant concern across digital channels. These unrequested messages, designed to promote goods, services, or brands, frequently flood inboxes, mobile devices, and other communication platforms. While businesses use them as direct marketing tools, their prevalence raises ethical and practical challenges, such as privacy violations, cluttered communication channels, and cybersecurity risks like phishing.

Table of contents

- [Introduction](#)
- [Definition](#)
- [Key Highlights of the TCCCPR Second Amendment](#)
- [End of Inferred Consent](#)
- [Compliant Mechanism](#)
- [Fines and Penalties](#)
- [Defense Strategies](#)
- [Country-Level Actions](#)
- [Conclusion](#)

Definition

According to Telecom Commercial Communications Customer Preference Regulations (TCCCPR), 2018, the term Unsolicited Commercial Communication refers to any commercial communication that does not align with the consent or registered preferences of the recipient. It excludes transactional messages or voice calls, service messages or voice calls, and communications issued under the directives of the Central or State Governments, constitutional bodies, or the Authority when in the public interest. Additionally, messages or voice calls transmitted under the Authority's explicit authorization are not considered Unsolicited Commercial Communication. Any communication from unregistered senders or those attempting to deceive recipients under the guise of commercial communication will be classified as Unsolicited Commercial Communication, addressing the misuse of telecom resources effectively.

Key Highlights of the TCCCPR Second Amendment

On 12 February 2025, TRAI introduced the Telecom Commercial Communication Customer Preference (Second Amendment) Regulations, 2025, refining the 2018 framework to tackle unsolicited commercial communications. The amendment, effective immediately except for certain provisions regarding the complaint mechanism starting 13 April 2025, implements several significant changes. Mixed promotional content is now considered promotional, necessitating pre-compliance, and new rules for auto-diallers and robocalls require prior notification to providers.

Government messages have been classified separately, exempting them from user consent while ensuring traceability through Distributed Ledger Technology to prevent misuse. Enhanced obligations for providers include authenticating and tracing communications, limiting senders to two telemarketers, and ensuring compliance with stricter regulations. Standardised agreements for providers, senders, and telemarketers reduce ambiguities and incorporate penalties for violations.

Additionally, a simpler complaint mechanism introduces a standardised format and response process with a 7-day user deadline, enhancing efficiency and accountability in addressing concerns related to Unsolicited Commercial Communications.

End of Inferred Consent

The 2025 amendment has abolished inferred consent derived from existing business relationships. Now, once a service contract ends, any promotional communication must stop unless fresh consent is obtained. This enhances consumer autonomy and reduces unsolicited contact. Businesses must obtain clear, verifiable consent before sending promotional messages. The amendment strengthens customer rights, combats unsolicited commercial communication, and mandates strict compliance through a strong framework. This shift reflects India's commitment to encouraging trust and transparency in customer

communication while reducing spam and misuse.

Compliant Mechanism

The recent amendments significantly boost consumer control over spam complaints. A key change is the removal of mandatory preference registration, simplifying the complaint process. Consumers now only need to provide basic information, such as their number, the sender's number, the message date, and a brief description, to report Unsolicited Commercial Communication. Additionally, the complaint window has been extended from 3 to 7 days, giving consumers more time to act.

Service providers are required to respond within 5 days, a major improvement from the earlier 30-day timeframe, making complaint resolution faster and more efficient. To deter repeat offenders, senders who violate the rules repeatedly may face blacklisting, telecom service disconnection for up to a year, and even device blocking. This introduces strong consequences for habitual spammers.

Additionally, consumers no longer need to manage separate preference registrations to control promotional messages. Every promotional communication must now include a clear opt-out option, ensuring consumers have straightforward control over the messages they receive. Together, these changes give consumers greater autonomy, faster complaint resolution, and stronger protection against spam.

Fines and Penalties

The Telecom Commercial Communications Customer Preference Regulations (TCCCPR), 2018, issued by the Telecom Regulatory Authority of India (TRAI) impose strict penalties to protect consumers from spam messages and calls. Unauthorised entities sending Unsolicited Commercial Communication can be fined up to ₹50,000 per violation, while registered telemarketers violating rules face graded fines starting from ₹1,000 for the first offence and up to ₹10,000 for repeat violations. Telecom service providers failing to act against offenders may incur penalties of up to ₹5,00,000 per contravention.

Entities using unregistered telemarketers for promotional communications also face penalties, with repeat violations resulting in stricter consequences such as blacklisting and telecom service disconnection. Persistent offenders can have their numbers or devices blocked to stop spam at the source. Consumers are empowered to report spam by forwarding messages to 1909 or using TRAI's DND app, with complaints resolved within five working days. These measures collectively aim to safeguard consumer privacy, reduce spam, and hold violators accountable through financial and operational penalties.

Defense Strategies

Telecommunication networks use technical measures such as caller ID and designated telemarketing numbers to tackle unsolicited communications. Additionally, consumer education campaigns through social media, institutional websites, and direct interactions effectively raise awareness about spam calls and messages. Many users proactively register their numbers with trusted organizations or national regulators to activate "do-not-disturb" services, which block unwanted calls and texts.

Country-Level Actions

National Regulatory Agencies (NRAs), in collaboration with stakeholders, employ public consultations, alerts, surveys, and meetings to mitigate unsolicited communication risks. These measures ensure well-informed regulations and safeguard consumer rights. Brazil has adopted a voluntary telecom industry code of conduct, while India uses blockchain-based solutions through TRAI to address nuisance calls.

India's blockchain-based Distributed Ledger Technology (DLT) framework under amended TCCCPR 2018 sets a global standard for combating Unsolicited Commercial Communication. By mandating the registration of communication templates on an immutable ledger, it ensures transparency, accountability, and explicit consent, reducing spam effectively.

In contrast, the US CAN-SPAM Act emphasises opt-out mechanisms, and the EU GDPR privacy Directive focuses on obtaining explicit consent, but both lack India's preemptive technological infrastructure. India's model bridges enforcement gaps by using blockchain for real-time consent verification and traceability, offering a scalable, tech-driven solution that can inspire global efforts to enhance consumer communication standards. After the pandemic, universal Internet access and inclusivity gained focus, but consumer safety and education on malpractices remain essential for creating a secure telecommunication environment.

Conclusion

Addressing Unsolicited Commercial Communication requires strong regulations, technological innovations, and consumer empowerment. The amended Telecom Commercial Communications Customer Preference Regulations (TCCCPR), 2018, strengthen protections through simplified complaint mechanisms, stricter penalties, and advanced traceability using Distributed Ledger Technology. Alongside regulatory efforts, public awareness campaigns and proactive consumer engagement play vital roles in combating spam and safeguarding privacy.

Collaborative measures involving regulators, telecom providers, and consumers ensure a secure and ethical communication environment. By embracing innovation and global best practices, nations can effectively curb Unsolicited Commercial Communication, encourage trust and ensure the integrity of digital communication platforms for all users.

For further details, write to contact@indialaw.in

Related Practice Areas

Consumer Dispute