09 October 2024

Jaipal Singh Tomar,
Advisor (QoS-II)
Telecom Regulatory Authority of India
Tower F, NBCC World Trade Centre,
Nauroji Nagar, New Delhi-110029

Subject: Tata Communications Limited comments to TRAI Consultation Paper on 'Review of the Telecom Commercial Communications Customer Preference Regulations, 2018'

Dear Sir,

This is with reference to the TRAI Consultation Paper dated 28-08-2024 on **'Review of the Telecom Commercial Communications Customer Preference Regulations, 2018.**

In this regard, please find enclosed herewith Tata Communication Limited's comments for your kind consideration as Annexure.

We request you to kindly consider our submissions while finalizing the recommendations and would be happy to provide any additional information, if required.

Thanking You,

Yours Sincerely,
For Tata Communications Limited,

Alka Selot Asthana
Vice President and Head Regulatory
(Authorized Signatory)

Enclosed: As mentioned above

Annexure-I

Tata Communications Limited's Response to TRAI Consultation Paper on "Review of the Telecom Commercial Communications Customer Preference Regulations, 2018 (TCCCPR 2018)"

At the outset, we thank TRAI for providing us an opportunity to share our comments/ inputs on this important paper pertaining to review of the present Telecom Commercial Communications Customer Preference Regulations, 2018 (TCCCPR 2018). In this paper the TRAI has raised the issues observed during the implementation of the regulations over a period of time and accordingly proposes necessary amendments.

In this paper, TRAI has carried out a comprehensive review of the existing regulations in terms of definition of transactional/ service communication, Complaint redressal mechanism, UCC detect system, Financial Disincentives, Differential tariffs and provisions related to registered senders & telemarketers. The comprehensive review of the regulation is of the steps taken by TRAI to curb the menace of unsolicited commercial communications (UCC).

Tata Communications Limited being a Telemarketer has a limited role in the entire value chain of stakeholders responsible for ensuring implementation and adherence of TRAI regulations, Directions and instructions issued from time to time on this issue. The Access Service Providers has a critical and major role in the entire ecosystem of curbing UCC. As a Telemarketer, our scope of work is specific to the extent of acting as bridge/ channel between the Telecom Access Service Provider and Principal Entity (sender) and execute functionalities prescribed under the Regulations in order to facilitate the promotional/ transactional communications for our Enterprise Customers. Therefore, in our response, we have concentrated on the issues concerning the Registered Telemarketers.

Our detailed issue wise response is as follows:

Q-1 Stakeholders are requested to submit their comments in respect of definitions of messages and calls and their categorizations, as suggested in the paragraphs 2.14 to 2.19 along with necessary justifications.

Tata Communications' Response:

We agree with TRAI proposal of change in the definition to introduce a mandatory opt-out mechanism from the inferred consent to the recipient in the same transactional message/call. This proposed change makes it clear that no mixing of commercial communication with transaction communication can be expected as there is now more clarity in the definition. Further, introduction of new category of communication "Government Messages / Calls" in addition to promotional and transactional category is also a welcome step.

It is also submitted that in addition to categorisation of the calls as per the defined category, a technical feasibility may also be explored to implement specific notification or color coding for each category of message/ call in collaboration with TSPs / Handset Manufacturers. This will enhance ease of convenience to the consumers to deal with each category of message/call.

Q-2 Whether explicit Consent be made mandatory for receiving Promotional Communications by Auto Dialer or Robo Calls? What can be other possible measures to curb the use of Auto Dialer or Robo Calls without the consent of the recipients? Stakeholders are requested to submit their suggestions quoting best practices being followed across the world.

Tata Communications' Response:

Yes, making explicit consent mandatory for receiving promotional communications through auto-dialers or robo-calls is a key step in protecting consumer privacy and reducing unwanted communication. Explicit consent means that consumers must clearly agree to receive such communications, typically by opting in through a specific action, such as checking a box or signing a consent form.

Global Best Practices for Managing Auto Dialer and Robo Calls

1. **United States: Telephone Consumer Protection Act (TCPA)**
    - **Opt-In Consent:** Requires businesses to obtain prior express written consent from consumers before making any promotional calls or sending text messages using auto-dialers or pre-recorded voices.
    - **Do-Not-Call Registry:** Consumers can register their phone numbers on the National Do-Not-Call list, which prohibits telemarketers from contacting them.
    - **Penalties:** Violations can result in significant fines, up to $1,500 per violation.
2. **European Union: General Data Protection Regulation (GDPR)**
    - **Explicit Consent Requirement:** Under GDPR, companies must obtain explicit consent before contacting individuals for promotional purposes, which includes auto-dialers or robo-calls.
    - **Right to Withdraw Consent:** Individuals have the right to withdraw consent at any time, and companies must make this process easy.
    - **Heavy Penalties:** Non-compliance can lead to fines up to 20 million euros or 4% of the global annual turnover, whichever is higher.
3. **Canada: Canadian Radio-television and Telecommunications Commission (CRTC)**
    - **Unsolicited Telecommunications Rules:** Require businesses to obtain express consent before using auto-dialers or sending unsolicited messages.
    - **National Do Not Call List (DNCL):** Similar to the U.S., this list allows consumers to opt-out of receiving marketing calls.
    - **Compliance and Penalties:** Non-compliance can lead to fines and penalties.
4. **Australia: Australian Communications and Media Authority (ACMA)**
    - **Spam Act 2003:** Requires businesses to obtain consent before making unsolicited commercial communications, including robo-calls.
    - **Do Not Call Register:** Allows consumers to opt-out of unsolicited marketing calls.

Suggested additional measures to Curb Unwanted Auto Dialer or Robo Calls

1. **Implement Advanced Caller ID and Call Blocking Technology**
    - Telecommunication providers can be required to implement technology that identifies and blocks spam or fraudulent calls before they reach consumers.
2. **Enforcement of Stricter Penalties**
    - Increasing fines and legal consequences for violations can act as a stronger deterrent for businesses that abuse auto-dialer systems.
3. **Require Real-time Identification and Disclosures**
    - Calls made by auto-dialers should include real-time identification of the caller, and an easy option for recipients to withdraw consent or report the call.
4. **Regular Audits and Compliance Checks**
    - Regulators should conduct regular audits to ensure compliance with consent requirements and actively monitor for violations.
5. **Public Awareness Campaigns**
    - Educate consumers on their rights and how to opt-out or report unwanted communications effectively.
6. **Technological Solutions for Consumers**

- Encourage the development and use of apps that filter or block unwanted calls and empower consumers to manage their own communications preferences more effectively.

Q-3 As most of the pre-recorded calls have pre-defined content, stakeholders are requested to comment on the process to be followed to scrub such content before the delivery to consumers. The comments should be supported with suitable justifications and practices being followed in other parts of the world.

Tata Communications' Response:

Scrubbing pre-recorded call content involves ensuring that the content is compliant with legal and regulatory requirements, relevant, and respectful to the recipient. This process not only protects consumers but also safeguards companies from legal repercussions.

In this regard, please find below a proposed comprehensive step-by-step process for scrubbing such content:

1. Content Review and Approval

- **Legal and Compliance Review:** All pre-recorded messages should be reviewed by legal or compliance team of Originating Access Service Provider to ensure compliance with provisions of TRAI Regulations (TCCCPR, 2018 as amended from time to time). This review should confirm that:
  - Explicit consent has been obtained from the recipient.
  - The message contains no misleading information.
  - The content respects consumer privacy and data protection laws.
- **Internal Compliance Team:** A dedicated team within the organization should be responsible for ensuring all messages adhere to internal guidelines and industry best practices.
- **Content Approval Workflow:** Establish a workflow for content creation, review, modification, and final approval, which includes multiple levels of review by legal, compliance, and marketing teams.

2. Pre-Screening for Sensitive Content

- **Identify Sensitive Topics:** Messages should be pre-screened for any content related to sensitive topics such as health, financial status, or personal information that could be deemed invasive or inappropriate.
- **Remove Personal Data References:** Ensure that no personal data or individually identifiable information is included in the pre-recorded messages without the explicit consent of the recipient.

3. Message Relevance and Context Check

- **Consumer Context Relevance:** The message should be tailored to the specific consumer segment and relevant to their relationship with the business (e.g., existing customers vs. prospects).
- **Avoiding Over-Communication:** Review the frequency and timing of messages to avoid consumer fatigue and annoyance, following best practices such as contacting during permissible hours.

4. Inclusion of Opt-Out Mechanisms

- **Clear Opt-Out Instructions:** All pre-recorded messages must include a clear and easy-to-understand opt-out mechanism, such as pressing a specific number to be removed from future calls.
- **Immediate Action:** Implement a process to ensure that opt-out requests are acted upon immediately to prevent further contact.

5. Compliance with Do-Not-Call Lists

- **Scrub Against National and Internal Do-Not-Call Lists:** Before delivery, scrub the call list against the national Do-Not-Call (DNC) registry and any internal DNC lists to ensure compliance.
- **Automated List Management:** Use automated systems to update and manage DNC lists in real-time.

6. Recording and Documentation

- **Document Review Process:** Keep detailed records of the review and approval process for each message. This documentation should include the content reviewed, the individuals who approved it, and the dates of approval.
- **Call Log Maintenance:** Maintain a log of all calls made, including the content delivered and any opt-out requests received.

7. Periodic Review and Updates

- **Regular Content Audits:** Conduct periodic audits of pre-recorded messages to ensure continued compliance and relevance.
- **Update Content Based on Feedback:** Use feedback from recipients and regulatory updates to modify and improve the content and delivery process.

Justifications and Global Best Practices

1. **Legal Compliance and Avoidance of Fines:**
    - **Justification:** Non-compliance with regulations like TCPA in the U.S. can result in significant fines and legal action. A robust content scrubbing process helps avoid such penalties.
    - **Best Practice:** In the United States, companies are required to have a comprehensive compliance program that includes reviewing all pre-recorded content for legal compliance before use.
2. **Consumer Trust and Brand Reputation:**
    - **Justification:** Scrubbing content ensures that businesses maintain a positive reputation and do not alienate consumers with inappropriate or irrelevant messages.
    - **Best Practice:** In the EU, under GDPR, explicit consent and relevance of communication are crucial. Brands that misuse pre-recorded calls can suffer both legal and reputational damage.
3. **Respect for Consumer Preferences:**

- **Justification:** Scrubbing ensures adherence to consumer preferences, reducing the risk of complaints and opt-outs.
- **Best Practice:** In Canada, compliance with the CRTC's unsolicited telecommunications rules requires clear and respectful communication, with an emphasis on honouring opt-out requests promptly.

4. **Operational Efficiency:**
    - **Justification:** A clear and structured process minimizes errors, reduces the risk of non-compliance, and streamlines content management.
    - **Best Practice:** In Australia, the Spam Act 2003 enforces strict rules on content and consent. Companies must have processes in place to ensure all communications are compliant and relevant.

Q-4 Stakeholders are required to submit their comments in respect of Headers identifiers categories as suggested in paragraphs 2.31 of Chapter II or any other type of identifiers which may facilitate consumers to identify senders distinctly. Suggestions if any, should be suitably brought out with necessary justifications.

Tata Communications' Response:

- **Labelling for Robocalls - Call Labelling Technology:** It is suggested to implement technology that labels calls as "Verified," "Spam," or "Scam Likely" based on the sender's information and behaviour. This helps consumers decide whether to answer.
- **Clear Opt-Out Mechanism:** Every message or call should include a simple and clear opt-out mechanism, such as "Reply STOP to unsubscribe" for SMS, or a keypress option for calls to end future communications.
- **Global Best Practices for Consumer Identification**
    - **European Union:** The e-Privacy Directive requires clear identification of the sender and opt-out options in every commercial message.
    - **Australia:** The ACMA enforces the Spam Act, requiring clear sender identification and opt-out mechanisms in all commercial messages.

We are of the view that by employing these identifiers and best practices, businesses can enhance transparency, ensure compliance, and build consumer trust while effectively delivering their commercial communications.

Q-5 Whether current provisions in the regulations for redressal of consumers' complaints in a time-bound manner are sufficient? If not, what provisions should be made for improving the effectiveness of the complaint handling processes including identifying and fixing the responsibilities of the violators?

Q-6 Whether facilities extended by the Service providers through Apps, Website and Call Centres for handling UCC complaints are accessible and consumer-friendly? Is there a need to add more facilities in the current systems? What measures should be taken by the service providers to make their Apps, Website and Call Centres easily accessible to the Consumers for registering UCC Complaints and tracking the same for a time-bound disposal of facilities needed.

Q-7 What additional modes of complaints registration, preference registration and consents registration through a very easy and quick process can be implemented?

Tata Communications' Response to Q5 to Q7:

Based on its experience and analysis, TRAI has carefully studied the existing provisions of complaint resolution and identified the areas of improvement. Certainly, the measures proposed to mitigate issues like delayed transfer of complaint from Terminating Access Provider to Originating Access Provider, high threshold to initiate an investigation against Unregistered Tele Marketer, provision related to action against UTM/ unregistered senders and no provision for misuse of 160 series etc. would lead to increased efficiency and promptness of actions to address customer complaints.

It is felt that there is a need to make the online channels - App/ websites etc. for creating more consumer-friendly interface in such a fashion that any voice call /SMS received from unsaved number should be followed by SMS from service provider wherein a link to complain against the number should be given with prefilled details of A number, time and date of call. The registration of complaint over e mail as a channel of complaint is a welcome step.

Further, it is felt that the current process of complaints is completely reactive, with AI, higher penalization, Opt-Out, and making the violator data public, UCC curbing can be controlled effectively.

Regulator Owned Caller ID and Spam Detection Mobile App

It is suggested that TRAI can implement a spam detection Mobile App with the following functions

- **Crowd-Sourced Caller Identification:** The app will maintain a global database of phone numbers and caller IDs, contributed by its user community. When a call is received, the app checks the number against this database and displays the caller's name, if available, even if the caller is not in the user's contact list.
- **Spam Labelling:** App uses data from user reports to label numbers as "Spam," "Scam," "Telemarketing," etc. This labelling helps users quickly identify if the incoming call is likely to be unsolicited or harmful**.**
- **Spam Score:** App assigns a spam score to incoming calls based on the number of reports and the type of activity associated with the number, giving users a clear indication of how risky the call might be.

Clear and Transparent Complaint Categories

- **Defined Categories**: Categorize complaints based on the type of violation (e.g., no consent, opt-out ignored, misleading content, etc.) to enable quicker identification and resolution.
- **Standardized Forms**: Use standardized complaint forms with predefined fields to gather all necessary information upfront, reducing back-and-forth communication.

Use of Advanced Technology for Complaint Management

- **AI and Machine Learning:** Use of AI can be initiated to categorize complaints, predict potential violations, and identify patterns of misconduct by analysing complaint data.
- **Automated Tracking and Alerts:** Systems can be implemented for automatically tracking of the complaints and for sending of alerts.
- **Accountability and Penalization Framework**
    - **Strict Penalties for Violators:** Imposition of strict penalties, including hefty fines, suspension of licenses, and blacklisting for repeated violations.

- **Public Disclosure of Violators:** Consideration of public disclosure of the names of entities with repeated or severe violations to deter future non-compliance.

Simplified Opt-Out and Consent Withdrawal Mechanisms

- **One-Click Opt-Out:** Consumers can be provided with easy and effective methods to opt-out of further communications, such as replying "STOP" to an SMS or pressing a key during a call.
- **Real-Time Update of Preferences:** It may be ensured that consumer preferences for opting out or withdrawing consent are updated in real-time across all telemarketers and operators.

Q-8 Stakeholders are required to submit their comments on the following

a. **Measures required for pro-active detection of spam messages and calls through honeypots and norms for the deployment of Honeypots in a LSA, and rules or logics required for effective use of AI-based UCC detection systems including training of AI models for identification, detection and prevention of spam**
b. **Proactive actions needed to stop further communications of messages or calls identified as spam through UCC detect systems and actions on the senders.**

Tata Communications' Response:

The proactive detection of spam messages and calls using honeypots and AI-based systems requires a multi-faceted approach involving strategic deployment of honeypots, ethical and regulatory compliance, advanced AI model training, and real-time detection mechanisms. By implementing these measures, it is possible to significantly reduce the incidence of unsolicited commercial communications, improve consumer experience, and enhance the overall security of communication networks.

The suggested deployment measures for Honeypots are as under:

- Deploy honeypots across various locations in a Licensed Service Area (LSA) to cover different network segments and user demographics.
- Use a mix of virtual and physical honeypots, including phone numbers, email addresses, and social media accounts, to capture a wide range of spam activities.
- Regularly change honeypot phone numbers and identifiers to prevent them from becoming known to spammers.
- Maintain a dynamic pool of honeypot resources that can be rotated to mimic real user behaviour and avoid detection by spammers.
- Honeypots should collect detailed logs of all incoming calls and messages, including caller ID, timestamp, message content, and call duration.
- Ensure data is collected in a structured format, making it easier to analyse and feed into AI-based systems.
- Ensure that honeypots are isolated from genuine user data to prevent any cross-contamination or accidental exposure of real user information.

Q-9 Stakeholders are required to submit their comments in respect of

a. **Financial disincentive proposed in Section F of Chapter II on the access providers against violations in respect of RTMs**

b. **Financial disincentive proposed in Section F of Chapter II on the access providers against violations in respect of UTMs**
c. **Financial disincentive against wrong approval of Headers and Message Templates proposed in Section F of Chapter II on the Access Providers.**
d. **Measures needed to assign the responsibilities of telemarketers (both RTMs and UTMs) and Principal Entities (Senders), involved in sending UCC and disincentivize them financially including legal actions as per law.**

Tata Communications' Response:

In this regard, we wish to submit that in the entire process of curbing UCC, punitive action should be determined basis the responsibility of the stakeholder(s) involved in the non-compliance towards TRAI Regulations. TMs is one of the stakeholders who merely act as a facilitator in the entire value chain and enables Sender (Enterprises) to use the same for sending communication. The Sender and DLT Platform are responsible to ensure compliance with the regulation and punitive action against RTMs is disproportionate.

Q-10 Whether there is a need to review five paisa exemptions accorded to transactional messages and bring them at par with other commercial messages? If yes, please give your answer with necessary justifications? If no, what additional measures are required to discourage senders, telemarketers or service providers from using transactional message templates for sending promotional messages?

Tata Communications' Response:

In our opinion, there should **not be any commercial exemption should exist between different type of messages**. Any such exemption gives rise to miscreant trying to take advantage of that commercial gap. Furthermore, for Access Service Providers, the utilization of technical resources doesn't change with type of messages. Therefore, the five paise exemption provided for transactional messages may be withdrawn in the revised framework of TCCCPR regulations.

Q11 Stakeholders are requested to offer their comments on the following issues:

a. **Whether there is a need to strengthen the provisions of Common Code of Practice templates with Standard Operating Processes further to enable Access Providers to take actions including imposing financial disincentives and actions as per law, against entities registered and not following the regulations? If so, what could be additional provisions and essential processes which should be made part of CoPs?**
b. **Whether there should be provision for minimum security deposits from the entities registering with any of the Access Providers, against the misuse or breach of regulations? If so, what should be the provisions in the CoPs for full or partial encashment/replenishment of security deposits against the breach of the regulations? Please provide your answers with suitable justifications.**

Tata Communications' Response:

The above measures to introduce financial disincentives and minimum-security deposits for telemarketers may result in preferential treatment of certain Enterprise customers or Telemarketers. Hence, we are of the view that such measures should not be adopted.

Further, as per the analysis carried out by TRAI in the consultation paper, it has come out very clearly that there is rising trend of complaint registration against the Unregistered Telemarketers. There is a need to take concerted efforts in order to reduce unsolicited calls/ complaints on account of unregistered telemarketers.

Q 12 What effective steps can be taken to control the menace of UCC through tariffs? Please justify your answer.

Q13 Whether differential tariff for SMS and Voice calls beyond a certain limit should be introduced to disincentivize UCC through UTMs? Please justify.

Q14 If differential tariff is introduced, what could be the limit beyond which differential tariff could be introduced for:

i. Voice Calls

ii. SMS.

Please justify with rationale.

Q15 If differential tariff is introduced, what could be the tariff beyond a limit for:

i. Voice calls.

ii. SMS.

Please justify with rationale.

Q16 Whether differential tariff should be introduced in a graded manner? If so, please suggest the methodology with justification.

Tata Communications' Response to Q12 to Q16:

We are of the view that TRAI should continue the tariff forbearance for SMS and Voice calls instead of introducing differential tariffs. The same should continue to be left to the market dynamics.

Further, it is pertinent to mention that as can be seen from the past precedence as well, TRAI had imposed SMS cap of 100 SMS per day which later has been withdrawn. We believe that recent steps taken by TRAI has observed reduction in the unsolicited calls / messages from the unregistered Telemarketers / Senders and with the amended TCCCPR Regulation, it will further strengthen the measures taken by TRAI to curb the menace of UCC.

Additional Comments

Comments on the Draft Regulation:

Reference 22 (4) (a) – "*Ensuring traceability of messages from Senders to recipients"*

> *a. There shall not be more than two TMs i.e. one Aggregator TM and one Delivery TM, or as directed by the Authority from time to time to allow sufficient flexibility in the eco system and at the same to maintain proper tracing and accountability of each entity in chain.*

Comment: TRAI in the above draft provision has proposed imposing restriction on up to two Telemarketers i.e. one Aggregator TM and one Delivery TM in the entire value chain which is not required and prohibit options available with sender to send its communications at affordable rates. The purpose of this proposed provision is to maintain proper tracing and accountability of each entity in chain. We believe that in current system as well, there is process in place to ensure traceability and accountability to identify non-compliant TMs. Therefore, we request TRAI to give adequate flexibility to Sender or delivery TMs to choose best available chain in the system to deliver the message at a competitive rate. Moreover, there are other various actions proposed in the regulation which ensure traceability of TMs by the Access Service Providers such as Annual verification, legal binding contract etc.

Issues faced by Enterprises/ TMs with Access Service Providers:

- No staging environment provided by Access Service Providers for DLT Platform to Enterprises for sanity check. Enterprises also needs to test their SMS templates to check if their content (including shortened URL) are complying to TRAI Direction in the DLT portal.
- Large pendency / delay in whitelisting the content templates and headers by Access Service Providers submitted by Enterprises. Access Service providers are giving priority and preference to large RTMs and Entities who are TSPs & RTMs for whitelisting of templates thereby giving them undue competitive advantage.
- In the process of whitelisting of the URL, few URLs are not going through on the DLT platform and giving multiple errors. TRAI should define TAT for Access Service Providers to resolve this issue to avoid any business impact / consumer issues for such impacted Enterprises.
- Increase in SMS size: With Sender ID addition, the SMS character limit may breach for certain message categories resulting in additional expense for Enterprises. For example, an SMS script currently having 158-character spaces will increase beyond 160-character spaces and will result in sending two SMSs instead of one SMS. This needs to be reviewed.
- Data synchronization of Content & Header in DLT platform takes lot of time and same is not happening in a uniform manner across all Access Service Providers and whitelisting time may vary from 2 hours to 6 hours for majority of instances. Moreover, a template rejected with a TSP is also approved by another TSP in some cases.
- Presently one of the TSP has introduced AI based solution in order to identify the promotional/spam calls. However, this is marking various genuine numbers also under spam category and the dedicated RTM from any company/Banks is unable to reach their customers. (subscriber will not answer the call, thinking it's a spam/promotional call)

Suggestions:

- Sender ID based binding should be implemented in a time bound manner to avoid fraud and misuse of the UCC Ecosystem. For example, if Enterprise has only registered with / selected TM "X" as its interface to send its communication, then, no other TM should be able to use the same sender ID.

- Access to DND complaints data base to TMs – There should be a provision in the regulation to provide access of DND complaint data base with TMs so that TMs will have flexibility to check the status of the complaint to ascertain that whether it's a genuine complaint or a fake. Example: A customer who has taken loan from a bank might raise a DND complaint in order to avoid such calls from the Bank. This will also help on faster resolution of complaints and reduce dependency on Access Service Providers.

.....